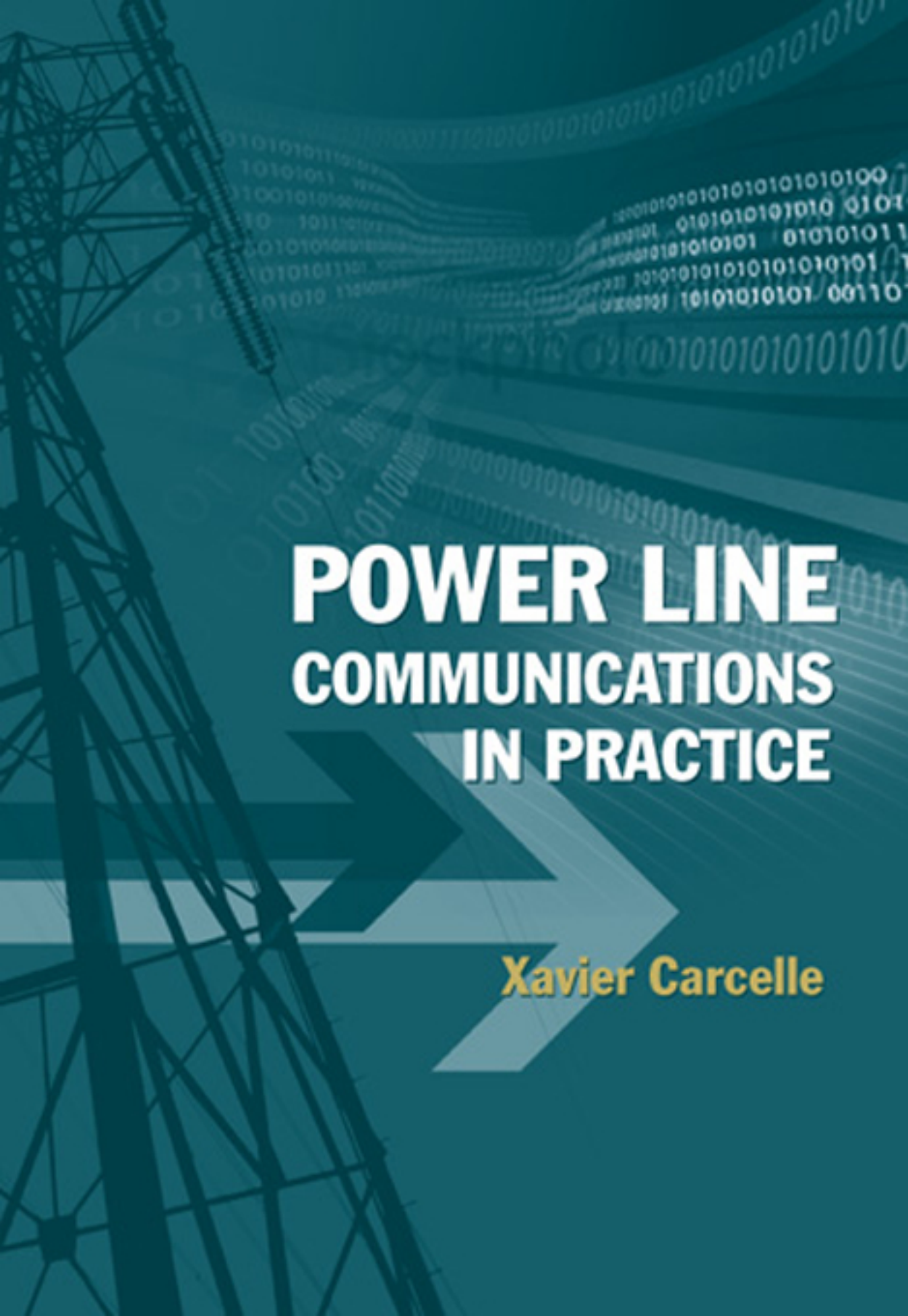
POWER LINE
COMMUNICATIONS
IN PRACTICE
Xavier Carcelle

Power Line Communications in Practice

For a listing of recent titles in the *Artech House Telecommunications Library*, turn to the back of this book.

Power Line Communications in Practice

Xavier Carcelle

ARTECH HOUSE
BOSTON | LONDON
artechhouse.com

Library of Congress Cataloging-in-Publication Data
A catalog record of this book is available from the Library of Congress

British Library Cataloguing in Publication Data
A catalogue record of this book is available from the British Library

ISBN 13: 978-1-59693-335-4

Cover design by Igor Valdman

Translated from the French language edition of: *Réseau CPL par la pratique* by Xavier Carcelle. ©2006 Groupe Eyrolles, Paris, France.

Ouvrage publié avec l'aide du Ministère Français chargé de la Culture—Centre National du Livre

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

10 9 8 7 6 5 4 3 2 1

To Yves, Françoise

Contents

Preface *xiii*

Organization of the Book *xiii*

Acknowledgments *xvii*

CHAPTER 1

Introduction 1

PLC Technologies 1
- Standard Organizations 2
- What Kinds of Standards Are There? 4
- Consortiums and Associations 8

Toward a Standardization of PLC Technology 10
- Future IEEE Standard **10**
- Future Interoperability Standard **10**

Advantages and Disadvantages of PLC 10

PART I

PLC Theory 13

CHAPTER 2

Architecture 15

Architecture of Electrical Networks 15
- Characteristics of Electrical Wiring 17
- Modeling Electrical Networks 22

Architecture with a Shared Medium 24
- Public Networks 24
- Private Networks 24
- Analogy with a Network Hub 25
- The Concept of PLC Repeaters 25

Layered Architecture 27
- The Physical Layer 27
- Frequency Bands 27

CHAPTER 3

Functionality 31

Network Mode Functionality 31
- Master-Slave Mode 32

Peer-to-Peer Mode 34
Centralized Mode 36
Transmission Channel Functionalities 38
Access to the Medium Using CSMA/CA Techniques 38
The ARQ (Automatic Repeat Request) Process 45
Synchronization and Frame Controls 49
Managing Frame Priorities 51
Managing Frequency Channels (Tone Map) 52
Segment Bursting and Contention-Free Access 53
Frame Level Functionalities 54
MAC Encapsulation 55
Fragmentation Reassembly 56
Other Functionalities 57
Dynamic Adaptation of the Bit Rate 58
Unicast, Broadcast, and Multicast 58
Service Quality 59

CHAPTER 4
Security 61

Overview of Network Security Issues 61
Cryptography 62
Public-Key Cryptography 66
Mixed-Key Cryptography 68
Electronic Signatures 68
Use of Public Keys 69
The Hash Function 69
Security for PLC Networks 72
Access to the Physical Medium 73
Access to Physical Frames 75
Authentication 75
Network Keys 75
Attacks 78
IEEE 802.1x and Improvements to PLC Network Security 80
Virtual Private Networks 85

CHAPTER 5
Frames 87

Physical Layer Frames 88
Architecture of the Physical and Data Link Layers of HomePlug AV 90
The OFDM Interface Frame 91
OFDM Symbols 91
Frequency Band Use for HomePlug AV Devices 93
Functional Blocks 94
Differences Between HomePlug Frames and 802.11b Frames 95
The PLC Physical Frame 96
MAC Layer Frames 100
MAC HomePlug 1.0 Frames 100

MAC Header Format 100
Format of an Encrypted MAC Frame 102
Format of Control and Management Frames 103

PART II
PLC in Practice 105

CHAPTER 6
Applications 107

Voice, Video, and Multimedia 107
Telephony over PLC 108
Visioconferencing and Videoconferencing 114
Multimedia 114
PLC Local Networks 115
Internet Connection Sharing 116
File and Printer Sharing 116
Audio Broadcasting 118
Recreational Applications 118
Video Surveillance 118
Backbone of a Wi-Fi Network 119
InternetBox and PLC 119
New Applications for PLC 121
PLC in Industry 121
PLC in Public Spaces 122
PLC over Coaxial Cable 122
PLC in Motor Vehicles 122
Economic Perspectives 123

CHAPTER 7
Equipment 125

PLC Technologies 125
Master-Slave Mode 126
Peer-to-Peer Mode 128
Centralized Mode 129
PLC Modems 130
PLC USB Modems 132
PLC Ethernet Modems 133
PLC Cable TV Modems 134
PLC Modems Integrated with Electrical Outlets 136
PLC/Wi-Fi Modems 136
Multifunction PLC Modems 137
PLC Audio and Telephone Modems 138
Methods for Accessing the Medium 140
Direct Tap Methods 143
Transformers and Meters 143
Transformers 144
Meters 144

Repeaters 145
Filters 146
The Cost of PLC 148

CHAPTER 8
Installation 151

Frequency Bands 151
Regulation of Radio Frequencies 152
Electromagnetic Compatibility and Frequency Bands 157
Topology of Electrical Networks 160
Single-Phase Wiring 161
Three-Phase Wiring 163
Wiring in an Electrical Network 164
The Circuit Breaker Panel 164
Attenuation on an Electrical Network 165
Choosing the Topology for a PLC Network 167
Propagation of the PLC Signal 168
Interference 169
Effects of Interference on the Electrical Network 169
Network Data Rates 171
Useful Throughput Calculation 171
Maximum PLC Actual Data Rate 175
Data Rate Variation 177
Security 178

CHAPTER 9
Configuration 179

Configuring a HomePlug 1.0 or Turbo Network 179
Configuring a PLC Network Under Windows 180
Configuring a HomePlug AV Network 187
Configuring a HomePlug 1.0 PLC Network Under Linux 191
Configuring a HomePlug AV PLC Network Under Linux 200
Configuring a PLC Network Under FreeBSD 204
Configuring an HD-PLC Network 205
Configuring a DS2 Network 206
Configuring Network Parameters 211
Review of Network Parameters 211
Configuring Network Parameters Under Windows XP 215
Configuring Network Parameters Under Linux/BSD 215

CHAPTER 10
PLC in the Home 217

Electrical Security 217
Choosing a PLC Technology 219
Choosing Equipment 219
Placing Devices on the Electrical Network 220
Configuring Security Parameters 223

Configuring the PLC Gateway 224
Configuring PLC Security 228
Testing Operation of the PLC Network 230
Firewall 231
VPN and PPPoE 232
Configuring an Internet Gateway 235
Sharing the Internet Connection 236
Configuring NAT and DHCP 237

CHAPTER 11
PLC for Businesses 247

Network Architecture 248
Supervising a PLC Network 249
Choosing a Standard 250
Choosing Network and Electrical Equipment 251
Service Quality 252
Access to the Electrical Medium 253
Placing Equipment 255
Choosing the Network Architecture 256
Security Parameters 257
Security Topologies 258
Configuring PLC Security 259
VLAN (Virtual LAN) 260
Virtual Private Networks (VPN) 260
Installing and Configuring a PLC Repeater (Bridge) 260
VoIP Under PLC 262
Sample Implementation of PLC in a Hotel 263
Network Implementation 263
Configuring a DHCP Client Under Linux 268
Configuring a DHCP/NAT Server 269
NAT (Network Address Translation) 270

CHAPTER 12
PLC for Communities 273

Electrical Networks for Communities 273
Electrical Network Operators 274
Topology of Electrical Networks 275
Topology of MV Networks 276
Implementation of a Communitywide PLC Network 277
PLC's Position Within the Network Architecture 278
Constraints of the Electrical Network for PLC Architecture 280
PLC Architecture 280
Issues in Electrical Networks 282
Choosing Equipment and Technologies 283
Supervision of the PLC Distribution Network 284
Configuring the Network 285
Examples of Small, Medium, and Large-Scale PLC Networks 287

CHAPTER 13
Hybrid PLC 295
Coexistence of Multiple Networks 295
PLC Technologies Between Themselves 296
Coexistence of PLC and Wi-Fi 298
Coexistence of PLC and Wired Ethernet 304
Advantages and Disadvantages of Network Technologies 304
Optimizing Network Architectures 304
Example of an Optimized Architecture 306
PLC and Wi-Fi, a Perfect Couple? 307

Resources 309
Web Sites 309
Books and Articles 311

About the Author 313

Index 315

Preface

Since the emergence of the first power line communication (PLC) products in early 2000, PLC technologies have been steadily undergoing great improvement, the aim of which has been to deliver optimum performance. Today, PLC has reached maturity and achieved performances comparable to the other LAN technologies, but with the added advantage of being much easier to deploy.

PLC makes it easier to broadcast any type of data within a whole building, including video over IP services proposed by the ISPs in their latest offerings. ISPs are willing to include the maximum number of IP applications in their offers on any type of terminal using the Ethernet interface to communicate with other terminals and the Internet.

The current lack of an IEEE standard imposes the HomePlug technology as a standard defacto, due to the amount of equipment already in use in the world (reaching 15 million at the time of printing). A working group at IEEE is about to finalize the first draft for a PLC standard with high performances, which is secure and complies with the EMC allowed in a domestic environment. The problem of interferences with Ham Radio technologies has been solved using a smart notching technique within the common sub-bands of frequencies.

The PLC devices' market will continue to grow in the near future with the integration of PLC interfaces (Wi-Fi, Ethernet, cable TV, and so forth) to be able to target the needs and aims of both network engineers and telecommunications companies.

Organization of the Book

This book presents the PLC technologies from all perspectives, ranging from the theory to the practical applications, in addition to being an installation guide for PLC networks targeting individuals, professionals, and corporations.

The author and the different contributors have produced the best pedagogical content enabling potential installers and users to master the techniques used in PLC technologies that are the nexus of electrical networks and computer networks. The many figures included in this book illustrate the different case studies, and exemplify the means by which network engineers can solve any problems arising while deploying PLC networks.

The book is divided into thirteen chapters, in two discernible parts:

- *Chapter 1. Introduction.* This first chapter covers the history of PLC technologies and presents the work carried out by the different working groups (alliances, industrial groups, and so forth) leading their development.
- *Part I. PLC Theory.* This part focuses on the characteristics of the electrical and computer networks and details the different functionalities proposed by PLC to stream the data by all possible means to the end user.
- *Chapter 2. Architecture.* This chapter describes the characteristics of the electrical networks by emphasizing their correlation with the common models used in telecommunications.
- *Chapter 3. Functionality.* The complete set of functionalities allowing the optimal data communications on the electrical network are listed in this chapter.
- *Chapter 4. Security.* PLCs do not suffer from the same security issues as do the Wi-Fi networks. However, some security measures have to be set up on PLC.
- *Chapter 5. Frames.* This chapter provides a complete description of the data frames transmitted on an electrical network.
- *Part II. PLC in Practice.* This part covers all the practical implementations of PLC, from the context of domestic users or professionals to Internet access networks for municipalities.
- *Chapter 6. Applications.* The current Internet access offered by the ISPs includes increasingly complex applications (voice, data, images, HD video streaming, and so forth) with good performances in terms of data throughput and security. This chapter illustrates how PLC networks can fulfill these requirements.
- *Chapter 7. Equipment.* The right choice of PLC equipment requires a good knowledge of the different functionalities implemented in PLC devices, such as gateways, filters, repeaters, and injectors, as complements to other network devices. This chapter provides criteria for making an appropriate choice depending on the function of the different installation constraints.
- *Chapter 8. Installation.* It is important to correctly configure the devices before installing them. This chapter deals with the problems of installation that usually arise in order to optimize the position of PLC devices on the electrical network.
- *Chapter 9. Configuration.* This chapter describes the different steps of configuration under different platforms (Windows, Linux, FreeBSD) and for different types of PLC technologies.
- *Chapter 10. PLC in the Home.* Individuals who would like to install a PLC network in their home will find all the information they need in this chapter, enabling them to make good choices. In addition, it provides advice on configuration and installation.
- *Chapter 11. PLC for Businesses.* From the SOHO to the large multi-site industrial companies, professionals will find detailed in this chapter the different steps to take in order to optimize the use of the electrical network as the backbone of their LAN.

- *Chapter 12. PLC for Communities*. This chapter focuses specifically on those communities faced with the issue of providing Internet access in remote areas. This chapter provides solutions and the architecture principles to be followed in a management project for Internet access using the public electrical network.
- *Chapter 13. Hybrid PLC*. This final chapter describes the differences between PLC and other network technologies and demonstrates how the best of each network technology in a LAN can be used to build up hybrid architectures that combine PLC, Wi-Fi, Ethernet, cable TV, and PSTN.

Acknowledgments

I would like first to extend my appreciation to the people at Artech and namely Simon Pluntree, my editor in chief, and Judi Stone, who have been following and supporting the project.

A great thanks goes to Michel Goldberg, whom I consider one of the best experts on standardization in the field of PLC networks. Michel reviewed the content of the book to ensure the quality of the first chapters and gave his great expertise to achieve such a book.

Florian Fainelli and Nicolas Thill, who are among the best Linux developers I know, helped me understand the frame controls for PLC networks from their Wi-Fi expertise in the OpenWRT project.

I am also indebted to the different people at the PLC devices' vendors and namely Werner Fehn at DEVOLO, Andy Barnes at Intellon, Terry Bernstein at Current, and Frederic Guiot at LEA.

The credits for the figures go to Marie-Helene Phuong for her incredible work concerning the graphic design based on my artwork. Her work will definitely help the readers to fully understand the principles of PLC networks.

CHAPTER 1

Introduction

The PLC (power line communication) designates a technology that uses the medium and low voltage electrical network to provide telecommunication services.

Although, since its first applications when the frequency range started at a low level, PLC is today more commonly used for high-frequency applications, also known as broadband powerline (BPL).

The electrical network has been used for a long time by producers and distributors of electrical power for the purpose of network monitoring and remote control at low speed.

Nowadays, an electricity producer or distributor cannot ignore standardization. It is interesting to note that the deployment of electrical networks, their interconnection, and the ever increasing number of electrical appliances have resulted in the emergence of the first network standardization bodies such as the IEC (International Electrotechnical Commission).

PLC Technologies

The principle behind the PLC technique is not one that has emerged recently. In 1838, Englishman Edward Davy proposed a solution allowing remote measurements to be taken of battery levels of sites far from the telegraph system between London and Liverpool. In 1897, he submitted the first patent (British Patent No. 24833) for a technique for the remote measurement of electrical network meters communicating over electrical wiring.

In 1950, the first PLC systems, known as Ripple Control, were designed and then deployed over medium- and low-voltage electrical networks. The carrier frequency was then between 100 Hz and 1 kHz. It was necessary to establish single-directional communications via control signals for the remote switching on and off of public lights or for tariff changes. The first industrial systems named Pulsadis appeared in France in 1960. The power involved was approximately a hundred kilovoltamperes (kVA).

Then the first CENELEC band PLC systems appeared, extending from 3 to 148.5 kHz, and allowing bidirectional communications over the LV (low voltage) electrical network, for instance, for meter readings (remote meter readings) as well as for a great number of applications relating to the home automation field

(intruder alarm, fire detection, gas leak detection, and so forth). Much less power needed to be injected, since the power was reduced to levels of approximately a hundred milliwatts.

The expression "power line carriers," usually abbreviated to PLC, appeared at the end of World War II in 1945. By that time, many telephone and electrical lines had been destroyed and there were more infrastructure electrical lines than telephone lines. For communication purposes, systems were designed for data transmission over high or medium voltage wiring by imitating remote meter readings already carried out on the electrical lines.

Figure 1.1 illustrates the changes in the PLC technologies classified by speed since the beginning of the 1990s.

Standard Organizations

The various standardization bodies as well as the concepts of standards and specifications which we will clarify are presented in this section.

The word "standard" covers several types of documents.

There is quite a difference between a norm and a standard, although, in English, most of the people use the same word: standard.

A "norm" is a document from an international body, such as the ISO (International Standardization Organization). It is sometimes called "standard *de jure*." In the following pages, we will call them "standard."

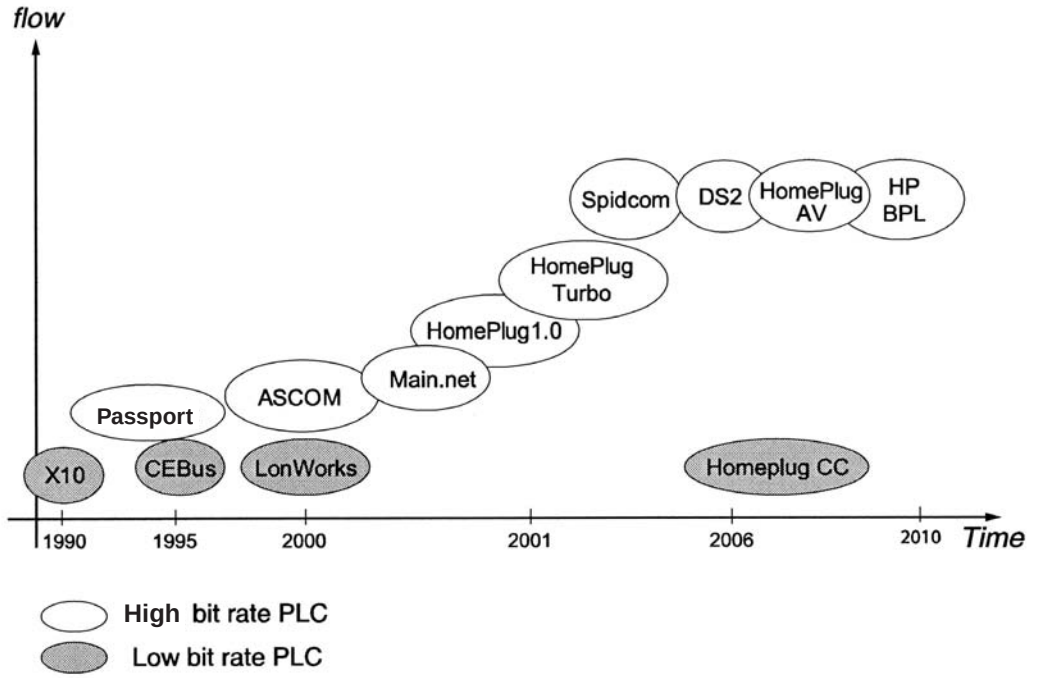

Figure 1.1 Low and high speed PLC technologies

A "standard" is a document from any national body, such as the IEEE (USA), or from a Community of States, such as ETSI. To make the difference, it is sometimes called "*de facto* standard." We will call it "specification."

To give a simple description of the conditions to be fulfilled by a standard, we refer to the definition given by ISO: "Any document designed for a repetitive action, and approved by an acknowledged standardization body and being at everybody's disposal." It is the result of a consensus.

Depending on the geographical areas, standardization work may be directly associated with an international level or first be developed at a regional level.

In Europe, standardization is carried out at national, European, and international levels. Each standardization committee is responsible for one or several standardization fields.

There are three international organizations that cover all the fields of knowledge: the IEC, the ISO, and the ITU.

The IEC (International Electrotechnical Commission) and Cenélec (European committee for electrotechnical standardization) are in charge of electrical engineering and the ETSI (European Telecommunications Standards Institute) is in charge of telecommunications.

The ISO and the CEN (European Committee for Standardization) cover all the other areas of activity.

The harmonized international standard terms are used in the background of so-called new approach European directives to designate European international standards adopted according to the general directions agreed upon between the European commission and the standardization bodies within the framework of a mandate granted by the commission after consultation with the member states.

Figure 1.2 illustrates the fields of activity of each standardization committee in charge of PLC technologies.

It must be noted that this regional level (here, the region is Europe) does not seem to exist explicitly in other parts of the world (Asia, the East, and so forth).

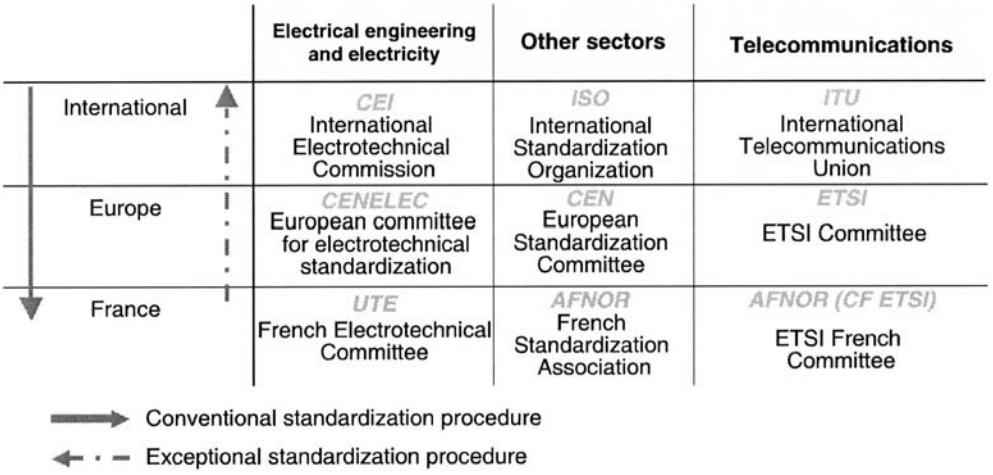

Figure 1.2 Standardization bodies in charge of PLC technologies

For European countries, this is a fundamental level since the international standards, the specifications of which will be used as a reference for CE marking, are written in the European standardization committees.

For a better understanding of the mechanisms for the implementation of international standards in a broad sense, this European standardization organization should be compared with the existing organization in the United-States.

Citing the "Overview of the U.S. Standardization System" (ANSI, Second Edition, July 2007), the United States is very different from other countries of the world, where usually one organization is designated as the major standards developer and that organization is closely tied to, if not a part of, the government. There are many organizations that comprise the U.S. standardization system, including both government and non-government organizations.

In the United States, there are essentially two broad categories of standards with regard to regulation—mandatory and voluntary. Mandatory standards are set by the government and can be either procurement or regulatory standards. A procurement standard sets out the requirements that must be met by government suppliers; regulatory standards may set health, safety, environmental, or other criteria.

VOLUNTARY STANDARDS—In the United States, the voluntary standards development system is called voluntary for two reasons. First, participation in the system is voluntary. Second, the standards produced are usually intended for voluntary use. Voluntary consensus standards are developed through the participation of all interested stakeholders, including producers, users, consumers, and representatives of government and academia.

In the United States, the distinction between voluntary and mandatory standards is not clear cut. Often, government standards developers refer in their regulations to privately developed standards, and in that reference give the standard the force of federal support. Building codes, for example, reference hundreds of standards developed by voluntary standards organizations. Since building codes are the province of government, the referenced standards have the force of law and must be adhered to by regulatory agencies such as the Federal Aviation Administration, the Environmental Protection Agency, and the Food and Drug Administration. The Department of Housing and Urban Development also references hundreds, if not thousands, of voluntary consensus standards in lieu of developing its own documents. These too, have the force of law once they are referenced in a government regulation. In the wake of the U.S. National Technology Transfer and Advancement Act (Public Law 104-113), which requires government agencies to use privately developed standards whenever it is at all possible, this practice is on the increase, saving taxpayers millions of dollars previously incurred by duplicating efforts in standards development.

What Kinds of Standards Are There?

There are at least four kinds of standards, based on the degree of consensus needed for their development and use, based on "The Handbook of Standardization" (ASTM, April 2006):

COMPANY STANDARD:
Consensus among the employees of an organization.

CONSORTIUM STANDARD:
Consensus among a small group of organizations, usually like-minded companies formed to undertake an activity that is beyond the resources of any one member. An example of a consortium is the United States Council for Automotive Research's (USCAR's) Strategic Standardization Board, which reflects USCAR's commitment to managing standards issues with regard to competitiveness.

INDUSTRY STANDARD:
Consensus among the many companies within an association or professional society. An example is a standard developed by the American Petroleum Institute (API), a trade association that is comprised of many different petroleum companies.

GOVERNMENT STANDARD:
May reflect many degrees of consensus. Some are written by individuals in government agencies, many are now being developed in the private sector and then adopted by reference as mandatory standards. Standards incorporated into federal regulations under the jurisdiction of the Environmental Protection Agency (EPA) or the Occupational Safety and Health Administration (OSHA) are examples of government standards.

According to the ISO, an international standard is "any document intended for a repetitive application, approved by a recognized standardization body and made available to the public."

Afnor completes this definition in the following way: "An international standard is reference information resulting from a carefully thought out collective choice to be used as an action base to solve repetitive problems."

We must point out that in relation to regulation, an international standard only defines methods and rules; therefore these are not mandatory, unlike regulations.

As indicated previously, for Europe, the regulatory framework is set by new approach directives which list the essential requirements that the product must meet. The harmonized European standards, when in compliance with their requirements, presumably ensure compliance with these essential requirements.

The importance of harmonized international standards is illustrated by the CE marking. This marking, which allows a product to be circulated freely around Europe, is a declaration from the manufacturer indicating that its product satisfies the essential requirements of the European directives concerning it.

The PLC equipment must satisfy the requirements of the EMC (electromagnetic compatibility) and LV (low voltage) directives.

A distinction should always be made between the work on the product and the work relating to the system, to the network in the case of PLC. To date, the work carried out on the product amends the CISPR 22, international publication, whereas, the work concerning the network is exclusively European and is dealt with by the Cenélec/ETSI Joint Working Group.

This work aims to make available a harmonized international standard on networks following the M 313 mandate given by the European commission to the

Cenélec and ETSI. This international standard is not aimed at limiting the deployment of wired networks but at limiting their interfering emissions.

After five years of trying to find a consensus, and noticing that it is almost impossible to define wired network radiation limits, it was decided to abandon the idea of publishing an international standard for this network, focusing instead on the international standard of the product.

In the meantime, in April 2006 the commission published a recommendation defining a legal framework at the request of the entire PLC community. This text recommends that member countries remove any barrier to the deployment of PLC networks; in return, the installers, equipment manufacturers, and Internet access providers undertake to comply with the requirements of the EMC directive and to use any remote mitigation method in the event of confirmed disturbance over a given frequency.

Extracts from the European Recommendation of April 6, 2005

1. Member States should apply the following conditions and principles to the provision of publicly available broadband powerline communication systems.
2. Without prejudice to the provisions of points 3 to 5, Member States should remove any unjustified regulatory obstacles, in particular from utility companies, on the deployment of broadband powerline communication systems and the provision of electronic communications services over such systems.
3. Until standards to be used for gaining presumption of conformity for powerline communications systems have been harmonized under Directive 89/336/EEC, Member States should consider as compliant with that Directive a powerline communications system which is:
   - made up of equipment compliant with the Directive and used for its intended purpose.
   - installed and operated according to good engineering practices designed to meet the essential requirements of the Directive.

   The documentation on good engineering practices should be held at the disposal of the competent national authorities for inspection purposes throughout the time the system is in operation.
4. Where it is found that a powerline communications system is causing harmful interference that cannot be resolved by the parties concerned, the competent authorities of the Member State should request evidence of compliance of the system and, where appropriate, initiate an assessment.
5. If the assessment leads to an identification of non-compliance of the powerline communications system, the competent authorities should impose proportionate, non-discriminatory and transparent enforcement measures to ensure compliance.
6. If there is compliance of the powerline communication system but nevertheless the interference remains, the competent authorities of the Member State should consider taking special measures in accordance with Article 6 of the Directive 89/336/EEC in a proportionate, non-discriminatory and transparent manner.
7. Member States should report to the Communications Committee on a regular basis on the deployment and operations of powerline communication systems in their territory. Such reports should include any relevant data about disturbance levels (including measurement data, related injected signal levels and other data useful for the drafting of a harmonized European standard, interference problems and

any enforcement measures related to powerline communication systems). The first such report is due on 31 December 2005.

8. This Recommendation is addressed to the Member States.

Done at Brussels, 6 April 2005 for the Commission, Viviane REDING, Member of the Commission.

At the Cenélec, the PLC guidelines are adhered to by the following technical committees (TC) and subcommittees (SC):

- TC 205, "Home and building electronic systems (HBES)";
- SC 205 A, "Main communicating systems";
- TC 210, "Electromagnetic compatibility (EMC)," CISPR mirror.

The mission of the SC 205, a "product" subcommittee, is to "prepare harmonized international standards for communication systems using low voltage electric lines or the building wiring as a transmission medium and frequencies greater than 3 kHz and up to 30 MHz. This task includes the allocation of frequency bands to transmit the signal over the low voltage network."

To comply with the IEC's nonduplication of work principle, the work on the *product* international standard is more or less pending in this subcommittee.

Figure 1.3 illustrates the various links between the parties involved (bodies, consortiums, states, European commission, and so forth) working on international

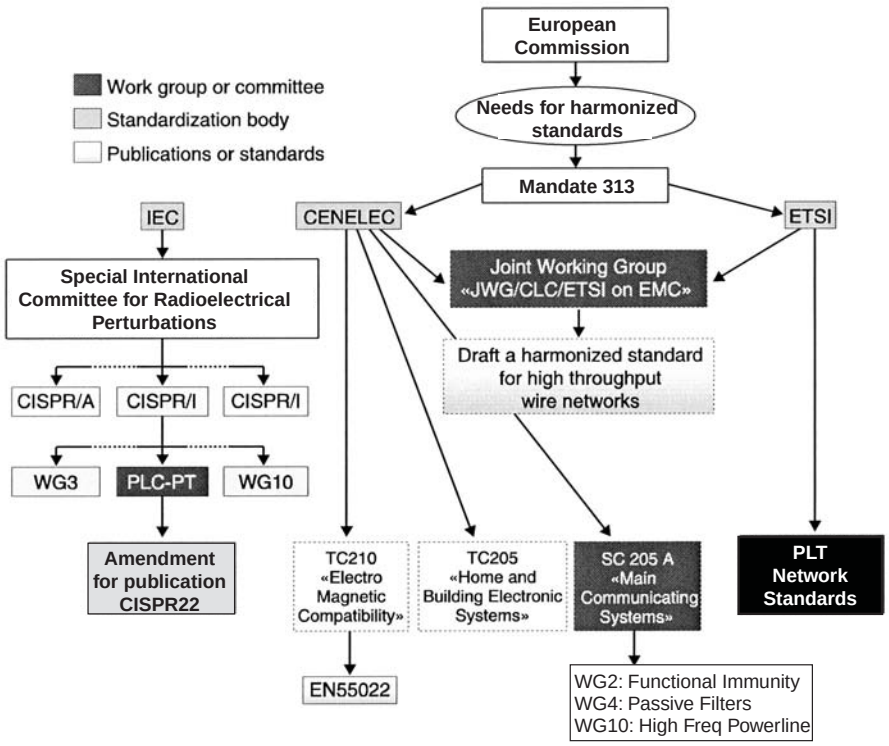

Figure 1.3 Parties involved in PLC standardization

and national standards relating to PLC in Europe, in particular the IEC, Cenélec, and the ETSI.

Consortiums and Associations

In addition to the bodies and institutions above, some associations and consortiums play a pre-standardization, or even standardization, role for PLC; in particular, the three major parties involved include HomePlug, the IEEE, and the Opera consortium. Historically in Europe, any lobbying in favor of PLC was conducted by the PUA and the PLC Forum.

Figure 1.4 illustrates the roles of each of the parties involved in this PLC pre-standardization.

HomePlug Alliance

Manufacturers for HomePlug Alliance groups cover both PLC technology and services in order to develop HomePlug specifications (HomePlug 1.0, HomePlug AV, and HomePlug BPL).

At present, only the HomePlug 1.0 specification has been finalized and implemented in many products on the market.

IEEE (Institute of Electrical and Electronics Engineers)

The IEEE, a non-profit-making body, is the largest technical international professional association and one of the main authorities for sectors as varied as aerospace systems, computers and telecommunications, biomedical technologies, electrical energy, or consumer electronics.

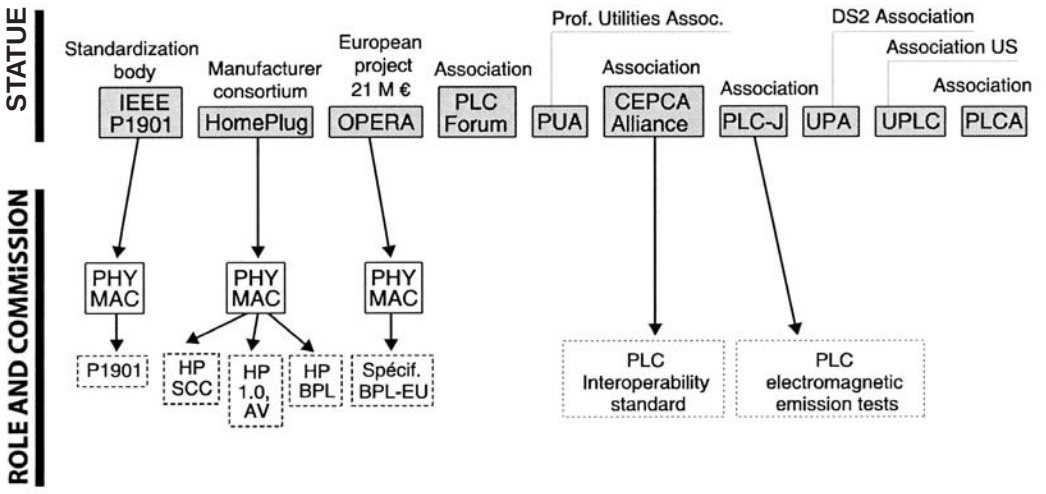

Figure 1.4 Consortiums and associations relating to PLC

The IEEE distributes both information and resources to its members, as well as providing technical and professional services. To stimulate interest in occupations related to the technology, the IEEE also offers services to its student members all over the world.

Another major aspect of the IEEE consists of prospects, individuals and corporations, buying its products and participating in its conferences and symposiums.

OPERA 2

The Opera consortium includes thirty-six partners native to various European countries and Israel. All the bodies and associations involved in the development of PLC technology are represented in the consortium, from public services to telecommunications operators through chipset makers, modem manufacturers, consultants, and universities.

This wealth of diverse profiles and skills plays an important role in the fulfillment of the consortium's objectives.

Opera's strategic objective is to "provide a high speed access service to all European citizens by using the most universal infrastructure—the PLC network." In order to achieve this, Opera carries out research and development, as well as demonstration and dissemination operations at a European level, so as to overcome any residual obstacle and to make it possible for PLC operators to provide high-speed access services to each European citizen at a competitive price.

The main Opera missions are the following:

- general improvement of low and medium voltage PLC systems (speed, easy implementation, and so forth);
- development of optimum solutions for PLC network connection to backbone networks;
- PLC system standardization.

PUA (PLC Utilities Alliance)

The PUA is an alliance created in Madrid on January 21, 2002, focusing on European public services delivering to more than a hundred million customers.

It currently has the following members:

- EDF (Électricité de France), France;
- Endesa Net Factory, Spain;
- Enel Distribuzione, Italy;
- Iberdrola, Spain;
- EDP (Electricidade de Portugal), Portugal;
- EEF (Entreprises Electriques Fribourgeoises), Switzerland;
- Unión Fenosa, Spain.

PLC Forum

The PLC Forum is an international body created at the beginning of the 2000s from the merger of two associations. It develops its activities in coordination with other bodies working on PLC.

Toward a Standardization of PLC Technology

Any standardization is a slow process. This is not surprising if we consider that it requires the consensus of the members of the particular work group before any decision is made.

Although this approach has proven to be efficient in most industrial fields, it is perhaps less suited to information technologies, the national standards of which should be aimed primarily at satisfying clients' immediate needs.

Future IEEE Standard

At the beginning of June 2005, the IEEE steering committee validated the creation of a draft PLC standard under the title "IEEE P1901 Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications."

The standard will apply to high throughput PLC equipment (greater than 100 Mbit/s at the physical layer level), in the frequency range lower than 100 MHz, and will address access techniques and internal networks. Furthermore, it will set out to define coexistence and interoperability mechanisms among the various items of PLC equipment, the quality of the service provided, and data confidentiality.

Almost all of the parties involved in PLC are involved in this project, in particular those listed in Table 1.1.

Future Interoperability Standard

An interoperability standard is being prepared to tackle multiple PLC specifications and technologies present in the domestic, professional, and public electrical networks.

Since the electrical network used as a communication medium is shared, these various technologies coexist on the electrical cables in the same frequency bands. Therefore, the various parties involved in PLC work together within the IEEE and CEPCA (Consumer Electronics Powerline Communication Alliance) to make them interoperable. This future standard is detailed in Chapter 14, which covers the prospects of PLC networks.

Advantages and Disadvantages of PLC

Like any viable system, PLC has both advantages and disadvantages in comparison with competitive technologies.

Table 1.1 Main Parties Involved in IEEE PLC Standardization

Advanced Communications Networks SA
Ambient Corporation
Arkados, Inc.
CEPCA Administration
Conexant Systems, Inc.
Corinex Communications Corporation
Current Technologies
DS2
Duke Power
Earthlink
HomePlug Powerline Alliance
IBM
IBEC (International Broadband Electric Communications), Inc.
Intel
Intellon Corporation
Itochu Corporation
Mitsubishi Electric Corporation
Mitsubishi Materials Ltd.
Panasonic Corporation
Pioneer Corporation
PUA
RadioShack
Schneider Electric Powerline Communications
SiConnect
Sony Corporation
Spidcom Technologies
Sumitomo Electric Industries, Ltd.
Texas Instruments
TEPCO
Toyo Network Systems Co., Ltd.
Universal Powerline Association
Xeline
Yamaha

Among the disadvantages, there is the relative immaturity of the products concerning the outdoor (external) and the access networks. In the case of high throughput, the problem is mainly related to the electromagnetic compatibility and compliance with emission constraints.

The main advantages of the PLC are the following:

- use of the existing electrical network, which involves potentially covering the entire country under consideration;

- quick deployment;
- no additional wiring;
- a robust encryption method.

PART I

PLC Theory

This part of the book is devoted to the HomePlug specification. Created by the industrial alliance of the same name, HomePlug focuses on two principal aspects: the physical layer, concerned with data transmission over the power line medium; and the data link layer, which defines the architecture and mechanisms to implement, allowing this transmission to take place over the network under the best possible conditions.

Since the release of HomePlug 1.0, two more versions have appeared, bringing improvements in transmission speed, security, and service quality.

To improve data transmission, the physical layer uses optimized techniques for coding, modulation, and error correction, resulting in excellent connectivity between devices and good transmission rates. The respective transmission rates for HomePlug 1.0, Turbo, and AV are 14 Mbit/s, 85 Mbit/s, and 200 Mbit/s, placing PLC in direct competition with Ethernet and Wi-Fi networks.

The data link layer implements a set of technologies providing excellent conditions for high performance transmission of data in the form of IP packets. The network access techniques that define this layer determine the network performance.

Successive releases of the HomePlug specification have improved this layer. Service quality has been optimized using time division multiple access (TDMA) techniques, and management of the network architecture of PLC devices has been refined through a hierarchal organization of data frames. Service quality is a key element for transmission of data in real-time applications, such as voice or video.

The difficulty of access to the physical medium under PLC provides increased immunity to attacks, yielding a higher security level that differentiates PLC from Wi-Fi. This immunity is further strengthened by the implementation of DES and AES encryption of frames transmitted on the power line medium, and by network integrity techniques that allow management of the devices authorized to participate in the PLC network.

CHAPTER 2

Architecture

PLC, or power line communication, is the generic name for a network technology that transmits data over electrical wiring. It is the result of extensive research on high bandwidth data transmission on the power line medium.

The architecture of PLC networks is comparable in many aspects to that of wired networks, but also to that of Wi-Fi networks, as we will see in this chapter.

HomePlug was the first PLC specification to provide a bit rate between 1 and 5 Mbit/s. Furthermore, HomePlug has implemented new techniques for connecting devices to the network, as we will examine in detail.

The HomePlug specification is in constant evolution. Multiple revisions have resulted in higher data rates, which remain limited by the shared nature of the medium. Additional improvements have been made in the areas of functionality, service quality, and security. The HomePlug alliance is currently the sole de facto PLC standard, but as we saw in Chapter 1, the ETSI (European Telecommunications Standards Institute) and IEEE have started their own standards processes.

This chapter introduces the overall architecture of PLC networks and provides detailed coverage of the two main layers: the physical layer and the data link layer.

Architecture of Electrical Networks

PLC (Power Line Communications) technology allows data transmission over electrical wiring. The electrical wiring is therefore the medium for data transmission, corresponding to the physical layer in the OSI model. Unlike other physical communication media like UTP (Ethernet cable), coaxial cable, fiber optic cable, and so forth, this role supporting data transmission is not the principal function of the electrical wiring. Data transport is therefore a complementary function to delivery of electrical power (approximately 110 V/60 Hz in the United States and Japan and 220 V/50 Hz in Europe) by the wiring that powers electrical devices from the public electrical network.

Electrical networks are classified according to their voltage level, as shown in Table 2.1.

This classification of electrical networks according to voltage levels allows the roles of associated organizations to be separated according to their area of responsibility.

Table 2.1 Levels of Electrical Voltage

Current name	*Traditional name (still in use)*	*Common voltage levels in France*
HV	Ultra high voltage	400,000V 225,000V
	High voltage	90,000V 65,000V
MV	Medium voltage	20,000V
LV	Low voltage	380V (three phase) 220V (single phase)

Drawing a parallel to the PSTN (public switched telephony network) model of a national telephone company, the electrical distribution network's power plant is its central office, supplying a distribution network that reaches all the way to the subscriber. This network is built on a star architecture where each branch of the star is the telephone wiring linking the subscriber to the central office.

In the PSTN network, the central office serves as a switch between the IP traffic coming from subscribers' modems in the 20 kHz to 1.1 MHz frequency band, and classic telephone communications in the 300 to 3,300 kHz band. Interpreted under a network model, the central office acts as an Ethernet switch and IP router to the high bandwidth link with the IP backbone (see Figure 2.1).

For example, in the French electrical distribution network, it is the MV/LV transformer that links the MT network and the distribution networks, each serving an average of 200 EDF subscriber meters (see Figure 2.2). The MV/LV transformer can be viewed as the Ethernet hub of the EGS network and the gateway to the IP backbone, on the basis of its high bandwidth IP transport links.

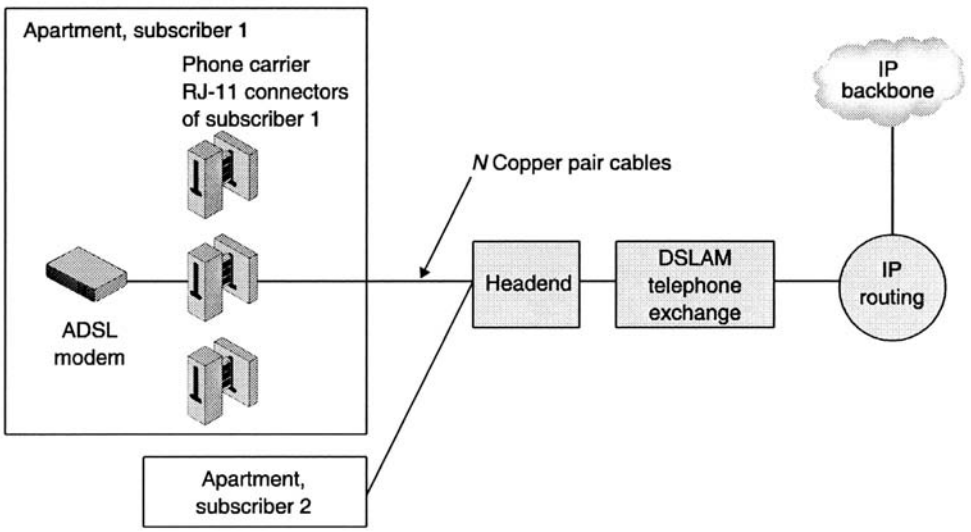

Figure 2.1 Simplified architecture of a PSTN (public switched telephony network)

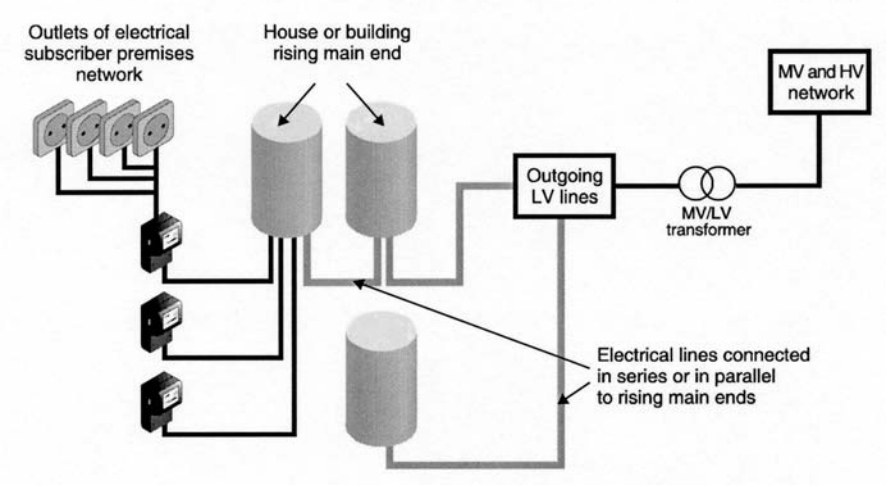
Outlets of electrical subscriber premises network
House or building rising main end
MV and HV network
Outgoing LV lines
MV/LV transformer
Electrical lines connected in series or in parallel to rising main ends

Figure 2.2 Simplified architecture of the electrical distribution network

In terms of responsibility, each part of the electrical network is operated by distinct organizations, responsible for supply and transport of electricity, as well as the transport of data in the case of PLC networks.

Figure 2.3 illustrates this division of responsibilities as applied to the different organizations composing the national electrical network.

Characteristics of Electrical Wiring

The physical support for communications based on PLC technologies is electrical wiring. It was not originally designed to transport data; its physical characteristics are primarily chosen to transport power at line voltage and frequency, such as 110 V/60 Hz.

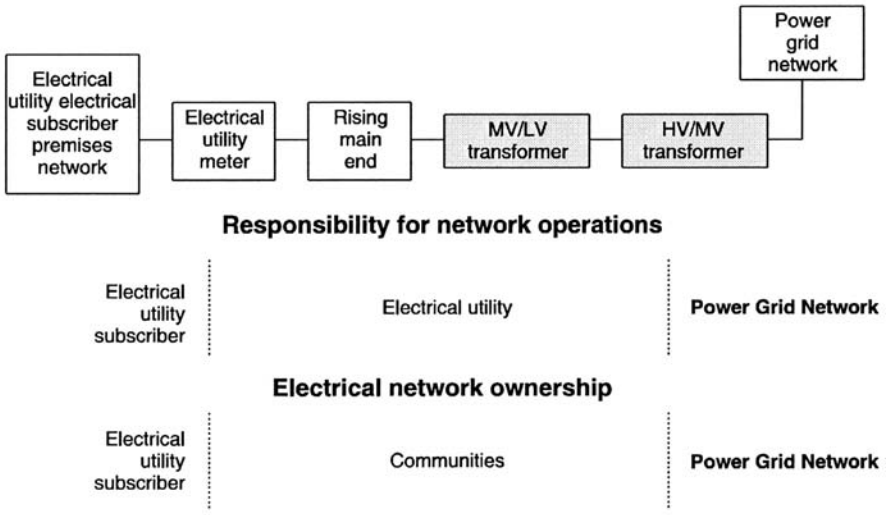

Figure 2.3 Operational responsibilities in the electrical network

This section introduces some of the physical properties of electrical wiring in order to understand its capabilities (both advantages and limitations) for the transmission of data.

Impedance

Electrical wiring is characterized by an impedance Z (the absolute value of the resistive, inductive, and capacitive components of the elements in the electrical network). It is not a fixed value. Devices are constantly being connected or disconnected from the electrical wiring. This modifies the wiring's impedance, making it difficult to model the communication medium, and therefore the transmission channel.

Additionally, the impedance of a device can vary as a function of its operating mode, speed, age, design, and so forth.

Studies have shown that the impedance of electrical devices powered by household electricity typically falls between 10Ω and 1 kΩ.

Capacitance and Inductance

The various devices connected to the electrical network all have a certain capacitance and inductance with regard to the electric current (110V, for example) that is present on the circuit, alternating at a line frequency of 50 or 60 Hz.

The *inductance* (L) of a circuit or electrical dipole, also called self-inductance, is a value that expresses the inductive flux created by the electrical current passing through it. The displacement of electric charges in a material having nonzero magnetic susceptibility (μ) creates a magnetic field (H) and a magnetic induction (B).

In the case of a material with a delimited surface, typically an electrical cable, the magnetic field produced by the current passing through the circuit creates an inductive flux. The inductance may be confined to the circuit or may interact with another electrical circuit.

The inductance can be expressed as a function of the magnetic field (ϕ) and electrical current (I) using the formula:

$$L = \frac{\phi}{I}$$

In the case of a sinusoidal voltage (as is the case for household electricity), this equation is expressed efficiently using Ohm's law as a function of the voltage (U), current (I), and frequency (f):

$$L = \frac{U}{2\pi f I} \text{ (expressed in henries)}$$

The *capacitance* (C), also called capacity, of an electrical circuit is a value expressing the potential energy stored in an electrical field created between two adjacent conductive surfaces of opposite electrical charge.

This potential energy, or capacitance, is proportional to the electrical charge stored by the electrical dipole formed by the two surfaces. This electrical charge can

also be expressed in terms of electrical flux (ϕ) and associated with the electrical potential between the two surfaces of the dipole:

$$C = \frac{\phi}{V} \text{ (expressed in coulombs)}$$

In the case of a sinusoidal voltage (as is the case for household electricity), this equation is expressed efficiently using Ohm's law, as a function of the voltage (U), current (I) and frequency (f):

$$C = \frac{I}{U2\pi f} \text{ (expressed in farads)}$$

The *impedance* (Z) of an electrical circuit is composed of resistive (R), inductive (L), and capacitive (C) components. Together, they completely characterize the impedance from an electrical point of view.

These characteristics have an influence on the overall behavior of the electrical network as a function of the electrical current flow in the network. From a computer science point of view, these characteristics compel a particular modeling of the physical layer in order to obtain the best quality possible from the transmission channel.

Using Ohm's law, the impedance may be expressed in complex values as the sum of resistive, inductive, and capacitive components, where j expresses the imaginary part of a complex value:

$$Z = R + jL2\pi f + \frac{1}{C2\pi f} \text{ (expressed in ohms for the absolute value)}$$

As the current passes through multiple electrical circuits, their combined impedances form a complex network of impedances in series and parallel. Sections may be connected or disconnected at any time. Also, the various impedances induce mutual magnetic and electrical fields that create electrical currents based on their relative proportions. From the point of view of a transmission channel, this property can have surprising implications, as we will see.

Since the inductive and capacitive characteristics constantly modify the physical transmission channel, PLC transmission techniques must be optimized and consolidated.

Electromagnetic Noise and Perturbations

The transmission channel acquires a certain noise level from the various electrical devices connected to the electrical wiring or in its proximity.

The different types of noise that can be identified on and around the wiring are:

- impulse noise from stops and starts of electrical devices;
- broadband white noise, whose power spectral density is the same at all frequencies;
- periodic noise at multiple frequencies;

- harmonic noise, composed of multiple frequencies used by electrical equipment connected to the network and which are multiples of the line frequency (for example, 50 Hz yields harmonics of 300 Hz, 600 Hz, and so forth).

Overall, the noise is quantified by the signal-to-noise ratio, or SNR, generally measured in decibels (dB).

In addition to noise on the power line medium, devices connected to the electrical network, or disconnected but located in proximity to the wiring, create a measurable level of perturbations on the transmission channel. This rather complex technical subject is known as EMC (electromagnetic compatibility).

From the EMC point of view, every powered electrical device generates electrical perturbations, which may be conducted (transported on the electrical wiring) or inducted (emitted in the radio environment of the device).

Numerous working groups in Europe (Cenélec) and internationally (IEC) have established rules that specify authorized limits for the perturbations produced by each category of electrical equipment, including PLC equipment. Also, telecommunications standards organizations in Europe (ETSI) and internationally (ITU) are studying perturbation thresholds in order to optimize the transmission channel, and signal processing techniques to obtain the best performance from PLC. The IEEE is also working on these issues to optimize the physical layer of the OSI model.

The ISRIC (International Special Radio Interference Committee) Working Group 3 has set allowable limits for perturbations from PLC electrical devices in the 150 kHz to 30 MHz band.

The EMC perturbations received and provoked by PLC are the subject of numerous other projects and studies. Their objective is to standardize emission levels of each device and to obtain a transmission channel that works efficiently with this level of emissions.

Attenuation

In the same way that a radio signal's power is and attenuated function of the distance traveled by the waves, or a DSL signal is attenuated as it travels on the PSTN's copper pairs, the electrical signal loses power as a function of the distance traveled.

This characteristic of electrical wiring must be taken into account when implementing a PLC network. In Chapter 8 (Table 8.10), we will study in detail the choice of parameters that offers the best performance for a PLC network. They vary greatly as a function of the range and attenuation of the signal.

Variations in impedance on the electrical network provoke effects such as multipath, giving rise to "notches" or amplitude peaks in the PLC signal, which may be considerable at certain frequencies. In the home, signal attenuation on electrical wiring is on the order of 20 to 60 dB, depending on the topology and content of the wiring network.

The minimum attenuation for the meter and circuit breakers combined is 30 dB for a system based on frequencies above 20 MHz. For frequencies below 20 MHz, the average attenuation is approximately 50 dB. However, a good PLC coupler can reduce the attenuation to 10 to 15 dB for certain frequencies.

The signal frequency of a HomePlug 1.0 modem is between 4 and 25 MHz, giving a power spectral density of –50 dBm/Hz. We will examine the consequences of this value in Chapter 8 (Table 8.10).

Table 2.2 summarizes attenuation values for the principal devices on the electrical network.

Multiple studies have shown that in a household electricity distribution network, the average signal attenuation is on the order of 50 dB/km.

Coupling Between Phases

When a high frequency alternating electrical signal is present on electrical wiring, it provokes a magnetic field, called coupling, in the proximity of the wiring.

The coupling is known as crosstalk when the induction is between components of the same electrical network and a telluric current when the components are in different networks.

Frequency Response

Depending on the nature of the electrical wiring (material, composition, age, and so forth), its response to a high frequency signal, that is, its ability to propagate the signal, varies considerably.

We will spell out the consequences of this characteristic for the implementation of a PLC network in Chapter 8 (Table 8.11), and show how they can be taken into account when choosing network topology and electrical cables.

Interface Sensitivity

Electrical devices contain analog interfaces that permit their coupling (inductive or capacitive) to the power line medium. In the case of PLC, these interfaces allow, among other things, the transmission of a digital signal over electrical wiring.

Table 2.2 Attenuation of Principal Electrical Equipment on an Electrical Network

Electrical equipment	*Attenuation*	*Comments*
Electromechanical meter	15 dB	Electromechanical meters attenuate the PLC signal but do not block it, resulting in propagation of the PLC signal outside of the private electrical network.
Electronic meter	15 dB	Equivalent to the electromechanical meter.
Circuit breaker	5 dB	If a signal linking two PLC devices passes through too many circuit breakers, it may be excessively attenuated.
Power strip	10 dB	The construction quality of the power strip has a great influence on its attenuation. Therefore, we should avoid connecting PLC devices to power strips.
Electronic meter and circuit breakers	20 to 30 dB	The meter and circuit breakers combined do not attenuate the signal enough to prevent its propagation outside of the private electrical network of a home or business.
Electromechanical meter and circuit breakers	30 dB	Above 20 MHz.
	50 dB	Below 20 MHz.

Depending on the electronic components used, the analog interface has a characteristic "sensitivity" that affects its ability to transmit the PLC signal without excessive degradation. This sensitivity is modeled by an impedance between the electrical wiring and the digital circuitry of the device.

Modeling Electrical Networks

Modeling an electrical network allows us to anticipate phenomena that occur during data transmission (perturbations, lost connections, and so forth) and to propose a representation that will best support the engineering of the network.

Whether electrical networks are considered in a public context (the case of electrical distribution networks) or that of a private home or business, modeling them is a difficult technical subject that requires consideration of numerous parameters (topology, nature of the wiring, perturbations, devices connected to the network, time of day, and so forth).

Since no tool exists for exhaustive modeling of electrical networks, the engineering of PLC telecommunications networks is limited to modeling the physical transport layer of the PLC signal.

Measurements carried out on electrical networks have allowed us to quantify the average impedance of an electrical line for high frequencies of the type used by PLC equipment.

Figure 2.4 illustrates the impedance curve in ohms (impedance as an absolute value) as a function of frequency. This impedance varies from 5 to 150 ohms for PLC frequencies.

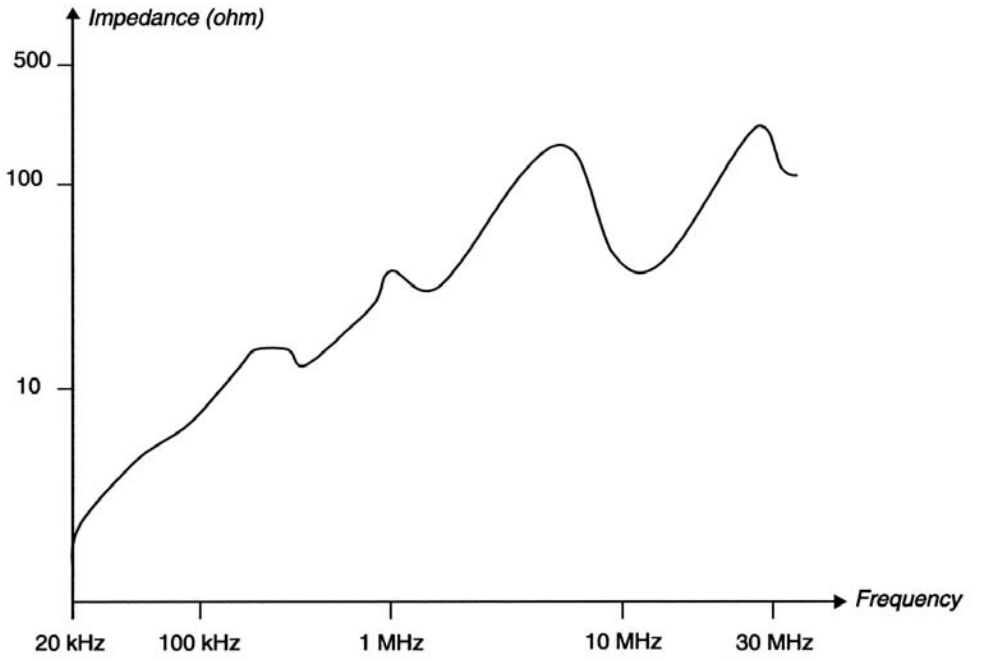

Figure 2.4 Average impedance of an electrical line as a function of frequency

Work by Nicholson and Malak has allowed us to express the average impedance of an electrical line by the formula:

$$Z_c = \sqrt{\frac{L}{C}}$$

where

$L = \mu H/m$ (linear inductance of the electrical line)
$C = \mu F/m$ (linear capacitance of the electrical line)

Work by Downey and Sutterlin has allowed us to model the electrical circuit equivalent to an electrical line. This circuit, composed of resistances, inductances and capacitances, may be schematized as shown in Figure 2.5.

The impedance of an electrical line is described by the following equation:

$$Z = R(f) + s \times L \text{ (expressed in ohms)}$$

where R is the resistance of the cable as a function of the frequency of the signal being propagated in the cable, s is the cable's diameter, and L is the line's inductance.

The impedance depends on the loads connected to the electrical line: electrical devices (hairdryers, halogen lamps, and so forth) connected to the network, each with a characteristic impedance.

These modeling elements allow us to calculate orders of magnitude for the characteristic values of electrical networks that affect the transport of PLC signals.

Modeling Electrical Devices on the Network

In the same way that it is difficult to model electrical networks, it is also difficult to model the electrical equipment connected to the network. This diverse equipment, constantly being connected or disconnected in unpredictable ways, causes continual variations in the network load.

Also, the equipment's characteristics vary according to its age, the time of day, the frequency of use, and so forth. As a result, such a model is rather imprecise.

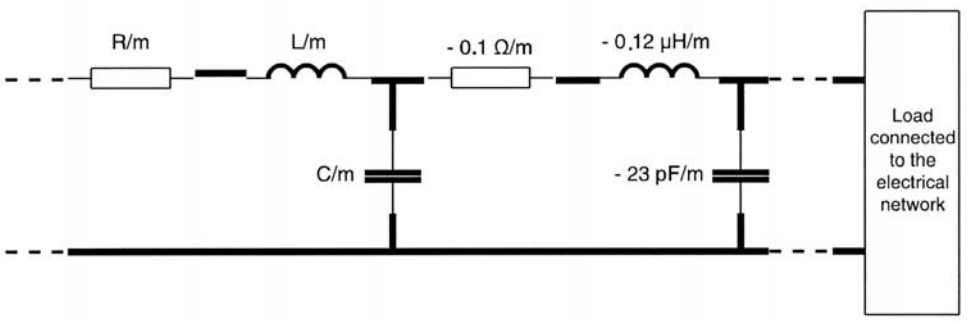

Figure 2.5 Schematic circuit of an electrical line as modeled by Downey and Sutterlin

With the exception of EMTP, which allows modeling an entire electrical network and all its wiring as a function of its topology, there exist few tools capable of facilitating the engineering and the understanding of the behavior of PLC signals on electrical wiring.

However, Cenélec (the European Committee for Electrotechnical Standardization) is developing a system to facilitate the modeling of in-home electrical networks.

Architecture with a Shared Medium

Chapters 10, 11, and 12 are devoted to the installation of PLC networks for homes, businesses, and communities. We will see that the topology of electrical networks can be viewed as a medium shared by all equipment carrying multiple PLC signals, transporting data exchanged between terminals of a local network.

In those chapters, we will distinguish "public" networks, which furnish electricity to individuals, businesses, and communities, and "private" networks, composed of the electrical distribution network of a building, from the meters to the outlets. We will see that the notion of a shared medium is equivalent to these two types of networks.

Public Networks

A public electrical network is a distribution network that supplies houses, apartments, buildings and businesses within a neighborhood, a town, or a community. This network is public to the extent that anyone may become a subscriber and be supplied by the local electrical authorities.

Figure 2.6 illustrates schematically a public electrical network supplying six meters, behind which we find PLC devices connected to the home's private electrical network. The medium is shared among the meters, according to the topology of the public electrical network (star, ring, and so forth) and its branches.

In this Figure, two electrical branches terminate at several meters and at PLC equipment. The PLC signal propagates between the various devices connected to the electrical network along these branches, including the sets of meter and circuit breakers. A related issue is the signal attenuation along the electrical wiring. We can thereby visualize the electrical network as a data bus, with PLC devices connected on both the public and private zones.

Private Networks

A private electrical network is located behind the meter connecting it to the public electrical network and is managed by those in the zone it serves: an apartment, a house, an office, a factory, and so forth.

The topology of this type of network, unlike that of public electrical networks, does not follow well-defined engineering rules and may be installation-specific (addition of parts of a network or circuit breaker panels, series topology, and so forth). Nevertheless, all branches of the network generally stem from the meter and

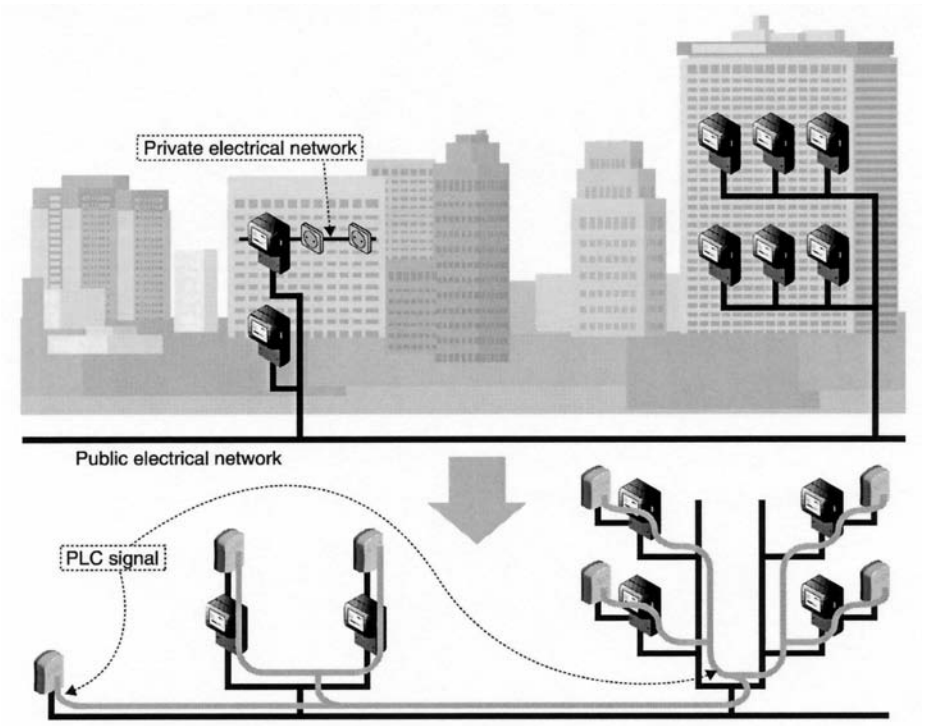

Figure 2.6 The public electrical network viewed as a shared medium

main circuit breaker panel, and the PLC signal circulates in all branches by passing through the panel.

Figure 2.7 illustrates a simplified example of an electrical network with three branches from the circuit breaker panel. On the right side of the illustration, the PLC signal propagates between all the outlets, thereby connecting the PLC devices. This example shows how a private electrical network can be viewed as a shared medium equivalent to a data bus.

Analogy with a Network Hub

The two preceding examples of public and private electrical networks demonstrate that any type of electrical network can be viewed as an immense data bus with the network's PLC devices connected to it.

In terms of telecommunications equipment, the most appropriate analogy is a concentrator or hub, with the various PLC devices connected to the electrical network representing different Ethernet ports.

Figure 2.8 illustrates this analogy schematically.

The Concept of PLC Repeaters

As we will see in Chapter 7, dedicated to PLC equipment, it can become necessary to repeat the signal in order to extend its coverage zone and to connect additional equipment.

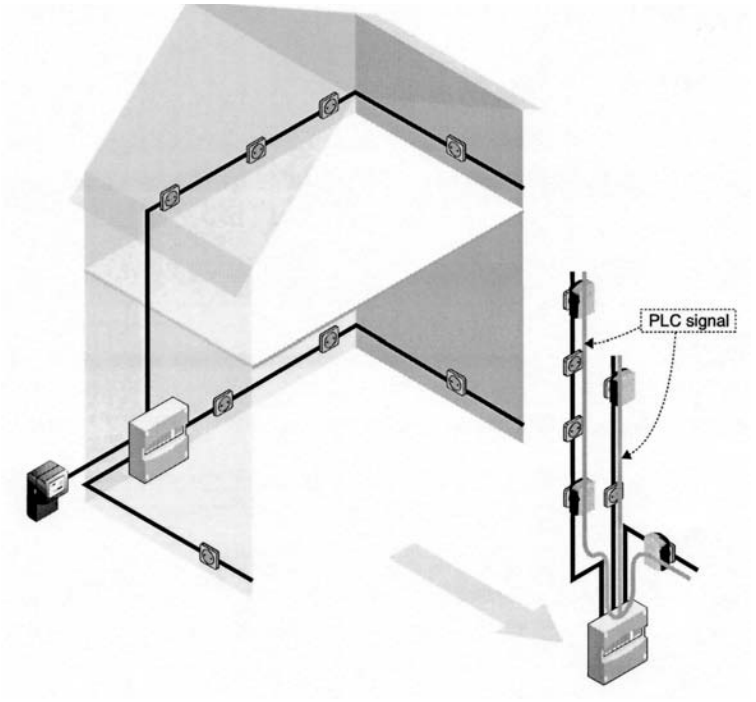

Figure 2.7 A private electrical network viewed as a shared medium

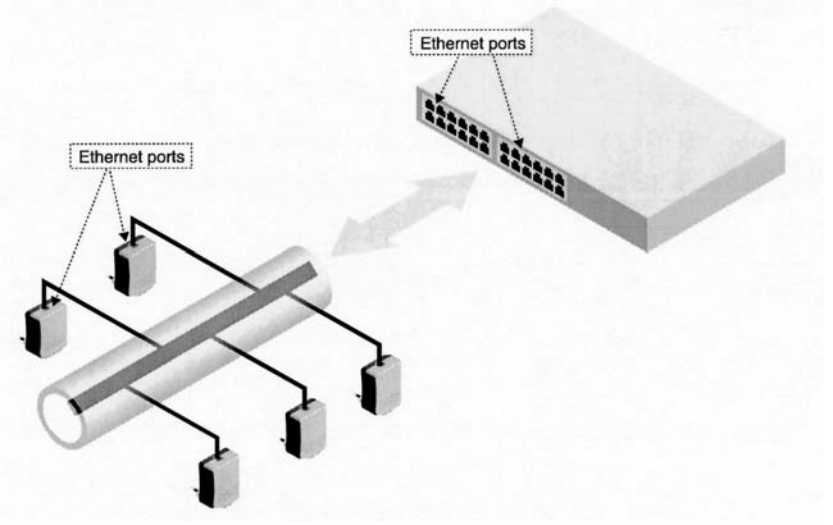

Figure 2.8 Analogy between a PLC network and a hub

At points in the electrical wiring where the PLC signal becomes too weak to be used by the network's PLC devices, the repeater amplifies and regenerates the signal.

Two different types of repeaters allow us to extend the range of PLC networks:

- "Physical" repeaters literally amplify the signal and retransmit it along the electrical line. This type is called physical because it operates on the physical

signal and not on the data frames. Therefore, this type of repeater does not reduce the bandwidth of the overall PLC network.

- "Logical" PLC repeaters repeat the signal at the level of the data frames. This type of repeater is composed of two PLC devices connected by their Ethernet interface. The first device is connected to one segment of the electrical network and the second device is connected to another segment that is inaccessible to the PLC signal due to excessive attenuation. This type of repeater reduces the bandwidth of the overall PLC network by a factor of two because it creates two distinct logical networks on the same physical electrical network.

Layered Architecture

The OSI (open systems interconnection) layered model provides a common base for the description of any data network. This model is composed of seven layers, each describing an independent protocol that furnishes a service to the layer above it and requests services from the layer below it.

In the context of this model, PLC networks correspond to layers 1 (physical) and 2 (data link), supplying an Ethernet connection service to the layers above.

Figure 2.9 illustrates the position of PLC technologies in the OSI model. Layer 1 (physical) is materialized by the electrical wiring that carries the PLC signal. The PLC equipment provides a terminal (typically a PC) with an Ethernet connection service corresponding to layer 2 (data link), using a MAC protocol and RJ-45 connectors. The terminal uses PLC network services to access services in higher layers (IP, TCP, HTTP, and so forth).

The Physical Layer

The physical layer of PLC technologies is materialized by electrical wiring and, more generally, by electrical networks. In order to transport the PLC signal on this medium, the line frequency (for example, 110 V/60 Hz) of the electrical circuit is supplemented by a modulated signal of low amplitude around a center frequency (carrier frequency) *F*.

The physical layer therefore consists of this low amplitude modulated signal, transported on electrical wiring at a frequency determined by the PLC technology employed and the applicable regulations. We will go into detail on modulation techniques in Chapter 3.

Figure 2.10 illustrates the sum of the PLC and power signals, which are superimposed on the electrical wiring, creating the physical layer of a PLC network.

Frequency Bands

The PLC signal is modulated in amplitude, frequency, or phase around a carrier frequency F. National or international standards organizations have set down rules that should be followed for the utilization of each frequency band, from zero to tens of gigahertz.

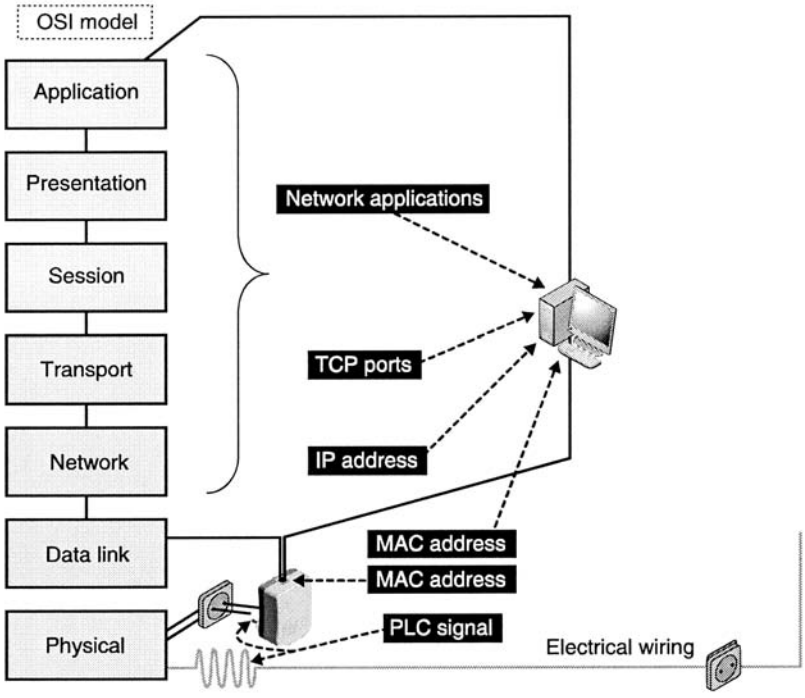

Figure 2.9 Position of PLC technologies in the OSI model

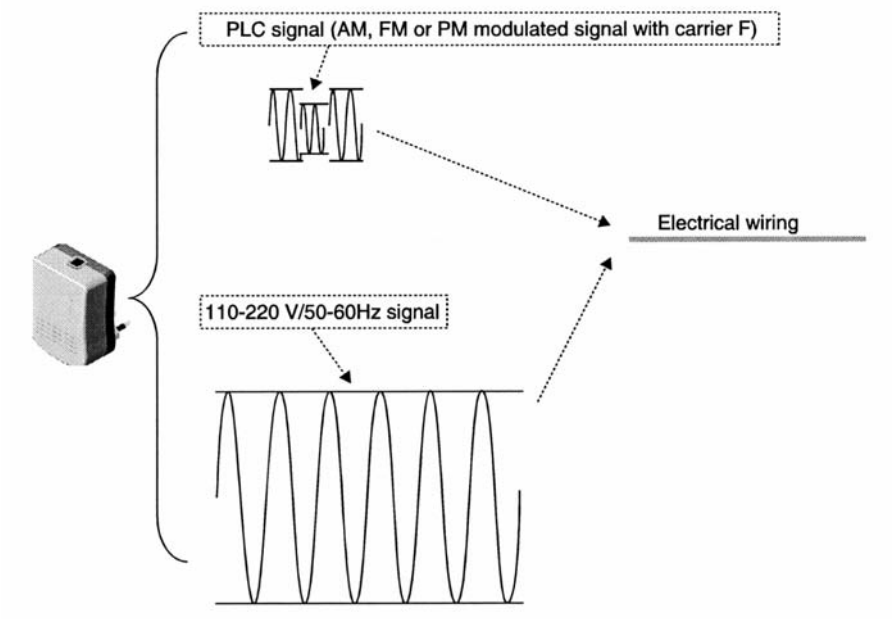

Figure 2.10 Sum of the modulated PLC signal and the power signal (for example, 110 V/60 Hz)

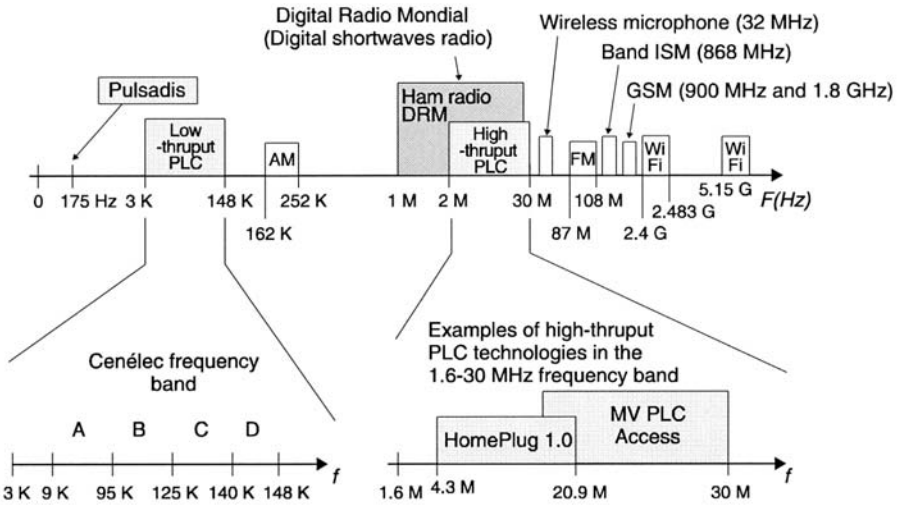

Figure 2.11 Frequency bands allocated to PLC networks

Two frequency bands are allocated to PLC technologies:

- 3 to 148 kHz for low bit rate PLC;
- 2 to 20 MHz for high bit rate PLC.

Figure 2.11 illustrates the placement of PLC frequency bands relative to those of other network technologies.

CHAPTER 3

Functionality

The functionalities of the PLC networks are introduced in this chapter. The technologies used in these networks are simple enough to be integrated into a single chip so that components can be manufactured at a very low cost. They will still be relevant up to the introduction of new PLC interfaces making it possible to increase the throughput of the devices.

The PLC functionalities take advantage of the many technological developments of fixed networks, in particular ADSL, Wi-Fi, Ethernet, and so forth. The PLC electrical component makes it necessary to employ technologies used to make the PLC link, which is the main weak point of this type of network, reliable.

The main functionalities of the PLC are the following:

- *network mode*, which is used to manage the network organization and communications between the various PLC devices;
- *PLC frame management mode*, in particular fragmentation and reassembly, which are used to solve the huge data volume transmission problem;
- *medium access technique*, which includes the synchronization of the network devices and priority management;
- *quality of service*, which authorizes the transmission of voice or video data in PLC environments.

Network Mode Functionality

One of the major functionalities of the PLC networks is the network mode, which is used to manage all PLC devices from the same network.

Since, by definition, a network consists of several devices exchanging data, it is necessary to implement an exchange management system so that they are organized and optimized.

There are several network organization methods. The various PLC technologies use one of the following three network modes:

- *Master-slave mode*. Can be compared to a client-server type IP network in which a master device manages the exchanges between the PLC devices of the network. The slaves can exchange data between themselves according to master management.

- *Peer-to-peer mode*. May be compared to a peer-to-peer IP network, where all the PLC devices of the network play the same role and have the same hierarchical level. These devices may have interchanges without being monitored by a master device.
- *Centralized mode*. Blending of the two preceding modes, in which a centralizing device is responsible for managing the network and exchanges between PLC devices. The other devices may also exchange with one another without having to go through the centralizer.

The main advantages and disadvantages of these three modes are summarized in Table 3.1.

Master-Slave Mode

The master-slave mode makes it possible to use the logic of the electrical network consisting of an electrical meter at the head of the network, which is considered as a master of the electrical network, its circuit-breakers and bus-bar connections, considered as slaves of these circuit breakers on which the PLC network is based for its physical medium and to place the so-called master device on the network head part and the slave devices on the various network strands.

In the case of PLC networks on public MV or LV electrical networks, the main functionalities expected from the master are the following:

- Management of the secured connections of the various slave devices. Each device belongs to a private logical network thanks to a dedicated connection channel on the electrical medium used as a shared medium. Therefore, the PLC frames circulate freely on the various strands of the electrical network.
- Management of the quality of service (QoS) of the PLC physical links between the slaves and the master by means of various physical level analysis methods (signal-to-noise level in each frequency sub-band, calculation of transmittable

Table 3.1 Advantages and Disadvantages of Master-Slave, Peer-to-Peer, and Centralized Modes

MODE	*ADVANTAGES*	*DISADVANTAGES*
Master-slave	— Centralized administration — Gateway role for PLC network — Management of Qos levels (TDMA) — Management of the roles of each device — PLC and IP network hierarchy — Easier network supervision	— Need for redundancy — Weak points concerning security — Possible bandwidth congestion — More complex configuration
Peer-to-Peer	— Bandwidth distribution — Distribution of PLC routing tables at a physical level — Easy to deploy	— No network hierarchy — Poor PLC gateway definition
Centralized	— Centralized administration — Only administration traffic passes via the coordinator	— Weak point on centralizer — Need for coordinator to manage TDMA frames

numbers of bits/Hz, and so forth). This QoS management is ensured by using a quality table for the various links located at the PLC master level.

- Possibility to create VLAN or slave inter-device links via the centralized administration of encryption keys at physical and possibly logical levels.
- Device supervision in order to integrate IP network administration tools (SNMP stack type) upstream in the PLC network according to a more complete IP network architecture.
- Management of the redundancy with other master devices.

The master device integrates in this way the entire PLC network intelligence providing optimized architecture management via embedded or remote interfaces accessible from standard protocols, generally HTTP or IP, with SNMP stacks permanently updated according to the fluctuations of the electrical network.

In the case of PLC networks on domestic LV electrical networks (apartment, house, SMB, hospital, hotel, school, and so forth), the functionalities expected from the various master PLC devices (there may be several devices on the electrical network in order to form a distinct logical architecture or to repeat PLC signals) are the following:

- Management of the quality levels of the PLC links between the slave devices and the master device as well as between slave devices.
- QoS management by means of the useful bandwidth parameters (concerning the TCP layer), of jitter and latency.
- Management of secured connections by using encryption keys for each logical network to ensure the logical isolation of each slave PLC device, for example in an architecture for a hotel or a university hall of residence. This functionality is used to detect newly plugged in or already plugged in devices.
- Management of the redundancy between master devices to ensure the correct operation of the entire PLC architecture with throughputs as high as 200 Mbit/s and still more in the years to come at the physical level.

Table 3.2 summarizes the main functions expected from the master PLC device and the corresponding technical solutions.

Table 3.2 Functions Expected from the Master Device and Corresponding Technical Solutions

FUNCTION	*TECHNICAL SOLUTION*
Frame collision	CSMA/CA
Time-division multiplexing	TDMA
Status table of physical links	"Tone Map" table
Synchronization of 50 Hz network frames	Zero crossing
SNR in each frequency sub-band	Listening to noise levels
MAC layer supervision	Frames and FEC
Supervision frames	Beacon regionalization and beacon mode

Peer-to-Peer Mode

The telecommunication network theory has been much based on the network device hierarchy principle. This principle was put into question with the emergence of ad hoc type architectures, either in wireless local area networks or networks for file exchange over the Internet, called peer-to-peer networks. The decentralized networks offer many advantages in comparison with hierarchical networks or networks in the master-slave mode.

In the PLC architecture in the peer-to-peer mode illustrated in Figure 3.1, all the PLC devices play the same role and permanently exchange a number of parameters in order to keep the network consistent. In the case of HomePlug 1.0, the devices exchange and update information locally.

The main parameters that the PLC devices require are the following:

- *Quality of the PLC link between a device and all the other devices*. This quality is assessed on a physical level in the same manner as radio devices assess the quality of the radio links to evaluate the available services in the upper OSI layers by means of a permanently updated table known as a tone map table.
- *EKS (encryption key select) encryption keys used to connect to a PLC network and for exchanges with other devices*. There are two EKS in HomePlug 1.0: DEK (default encryption key) and NEK (network encryption key). We'll cover their characteristics again in Chapter 4, which covers security and their configuration is covered in Chapter 9. These keys are used to create, over the same electrical network, several PLC networks in the peer-to-peer mode without communicating internetwork data. Since these networks use the same electrical network, the data communication throughput may be reduced as the PLC technology uses all of the 2 to 30 MHz frequency band.

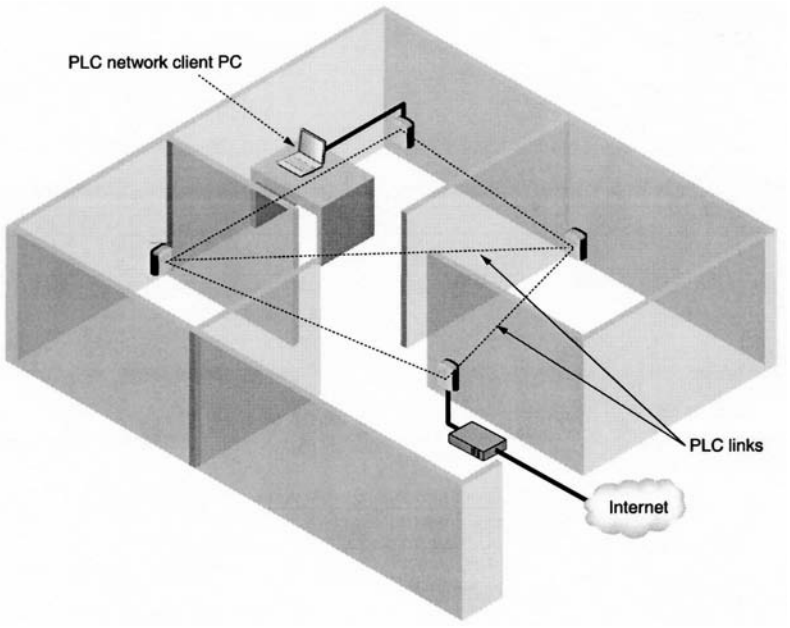

Figure 3.1 Architecture of a PLC network in the peer-to-peer mode

- *Selection of the best suited modulation mode and FEC (forward error correction) type in view of the PLC link qualities*. In the case of HomePlug 1.0, the four possible modes are DQPSK ¾ (differential quadrature phase shift keying), DQPSK ½, DBPSK ½ (differential binary PSK), and ROBO (robust OFDM), which are used to obtain four types of data rates.
- *Priority of each network PLC device*. This parameter is indicated in the VLAN field of the Ethernet frames for each PLC device according to its configuration. It is used to establish almost a network hierarchy with devices acting as gateways to other networks and other devices playing standard roles in the architecture.

Figure 3.2 illustrates the architecture of a PLC network in the peer-to-peer mode, in which these four parameters are permanently exchanged by the network devices in order to keep the network homogeneous and to maintain a better Ethernet frame and bandwidth routing distribution.

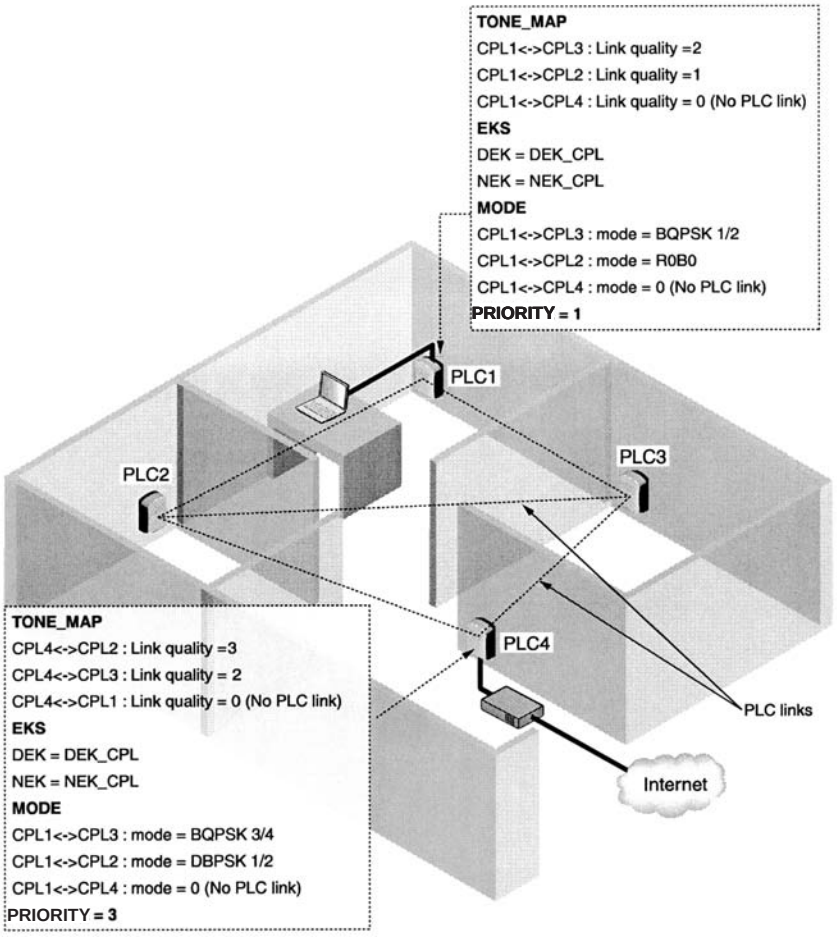

Figure 3.2 Parameter exchange between PLC network devices in the peer-to-peer mode

HomePlug 1.0 PLC Network Hierarchy by Means of Priorities

Within IEEE 802.3 Ethernet frames, a VLAN field may be placed described in the IEEE 802.1Q standard. Within the framework of PLC networks in peer-to-peer mode, this field is used to create almost a hierarchy between the PLC devices of the same network. The field is encoded on 3 bits and therefore can have eight values.

Table 3.3 lists the four available PLC priorities according to the value of the VLAN field.

It may be useful to implement a higher priority on a PLC device used as a gateway to another IP network or being connected to a device of the server type liable to receive much traffic from the other network PLC devices connected to the PC in the client mode of said server. Several PLC devices connected to IP telephones over the network and having priority 4 to provide the best transmission time for real-time audio communications may also be possible.

This priority is one of the most important PLC network configuration parameters in the peer-to-peer mode, even though it is only a logical parameter that has no influence on the PLC links at a physical level. We'll cover this parameter again in Chapter 9.

The peer-to-peer mode is widely used in PLC networks complying with the HomePlug 1.0 standard, since PLC networks in which each device creates PLC links with devices connected to the other sockets of the electrical network can be quickly created with it. This mode is thus used to create a PLC ad hoc network over the electrical architecture of the building for the application requirements of the local area network.

The configuration and the optimization of the PLC network depend on the functionalities anticipated on the local area network and on the requirements in terms of client-server architecture in order to achieve a realistic architecture with regard to the performance of the PLC technologies.

Figure 3.3 illustrates the various steps in the organization of a PLC network in the peer-to-peer mode from the functionality requirements to the technical solutions.

Centralized Mode

The architecture of the HomePlug AV PLC technology is actually neither in the peer-to-peer mode nor in the master-slave mode. It involves two device types: devices with a similar hierarchical level and a centralizing device, as illustrated in Figure 3.4.

The CCo (central) device manages medium access allocations for the various PLC devices that want to communicate between themselves.

Table 3.3 PLC Priorities of VLAN Field

PRIORITY	*VLAN FIELD VALUE*	*APPLICATION CLASS*
Priority 3	7,6	VoIP (less than 10 ms transmission time)
Priority 2	4,5	Video over IP (less than 100 ms transmission time)
Priority 1	2,3	Raw data transfer and control traffic
Priority 0	0,1	Limited data communication

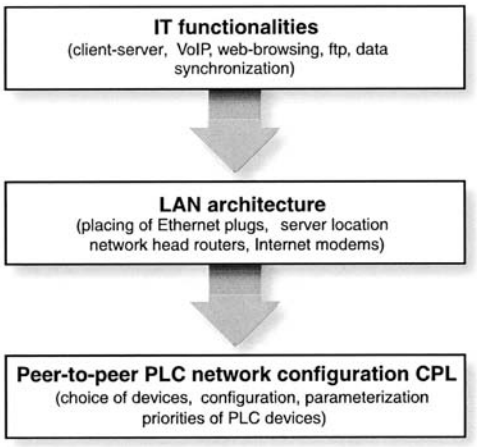
IT functionalities
(client-server, VoIP, web-browsing, ftp, data synchronization)
LAN architecture
(placing of Ethernet plugs, server location network head routers, Internet modems)
Peer-to-peer PLC network configuration CPL
(choice of devices, configuration, parameterization priorities of PLC devices)

Figure 3.3 Organization of a PLC network in the peer-to-peer mode

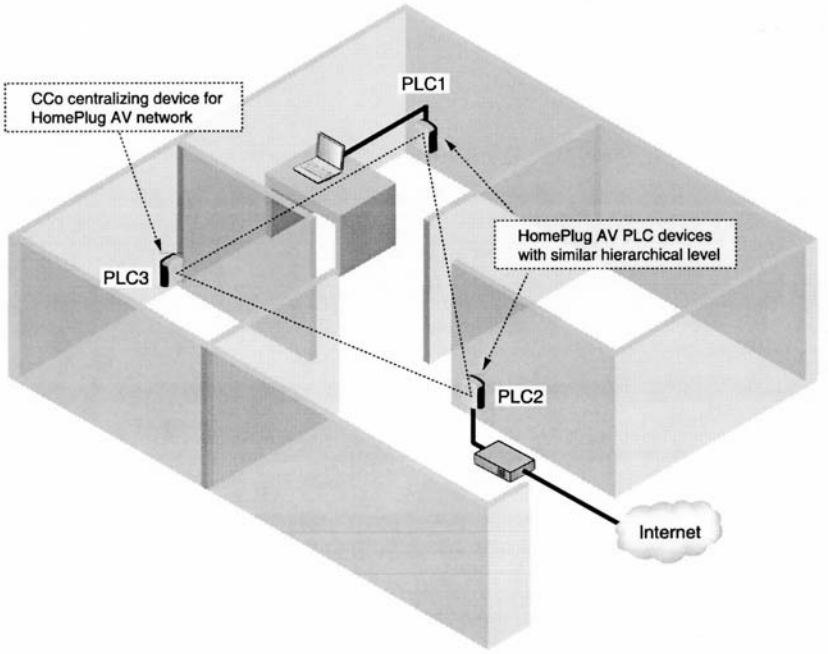

Figure 3.4 Architecture of a PLC network in centralized mode

The data is communicated between the PLC1 and PLC2 devices in the following way:

1. PLC1 and PLC2 put in place an estimate of the transmission channel (modulation levels, error coding level, and so forth).
2. PLC1 and PLC2 inform CCo (PLC3) that they wish to exchange data.
3. CCo (PLC3) allocates to them a time interval during which they have access to the medium.
4. PLC1 and PLC2 directly exchange their data without going via CCo.

If managing the medium access is handled by the CCo centralizing device like in the master-slave mode, the data is exchanged directly between the devices as in the peer-to-peer mode.

Transmission Channel Functionalities

In PLC, the transmission channel is the electrical network. Since it was not originally designed to support network applications, network functionalities had to be added to so that the data link layer could be implemented correctly. Among them, medium access and frame synchronization and frequency channel management processes on the electrical wiring are specific to PLC technologies.

Access to the Medium Using CSMA/CA Techniques

CSMA/CA (carrier sense multiple access/collision avoidance) is a so-called random access technique with listening to the carrier wave, which is used to listen to the transmission medium before sending data. CSMA prevents several transmissions from taking place over the same medium at the same time and reduces collisions but does not prevent them completely.

In Ethernet, the CSMA/CD (carrier sense multiple access/collision detection) protocol controls access to the medium of each station, and senses and handles the collisions that occur when two or more stations try to communicate simultaneously via the network.

In the case of PLC, the collisions cannot be detected. To detect a collision, a station must be capable of listening and transmitting at the same time. In PLC systems like in radio systems, the transmission prevents the station from listening at the same time at the transmission frequency. Because of this, the station cannot hear the collisions. Since a station cannot listen to its own transmission, if a collision occurs, the station continues transmitting the complete frame, resulting in a global loss in network performance.

With these specific characteristics in mind, PLC uses a slightly modified protocol compared with CSMA/CD, called the CSMA/CA protocol. The role of CSMA/CA is not to wait for a collision to occur to react as with CSMA/CD but to prevent collisions. Therefore, CSMA/CA tries to reduce the number of collisions by avoiding their occurrence, knowing that a collision is most probable when the medium is being accessed.

To avoid collisions, CSMA/CA uses various techniques, such as medium listening techniques introduced by the PLC; the back-off algorithm for medium multiple access management; an optional reservation mechanism, the role of which is to limit the number of collisions by making sure that the medium is free; and positive acknowledgment (ACQ) frames.

The CSMA/CA used in the PLC is slightly modified compared with the one used in Wi-Fi. Using a value that indicates the number of times that a station could not emit in comparison with other PLC stations with the same medium access priority is specified in the HomePlug standard. This value, called DC (Deferral Counter),

increases when a station could not emit, making it possible to bring the use of the network in line with this priority level.

Figure 3.5 illustrates the operation of the CSMA/CA algorithm in its entirety.

Listening to the Medium

In PLC, the medium is listened to both at the physical layer level with the PCS (physical carrier sense) and at the MAC layer level with the VCS (virtual carrier sense).

The PCS makes it possible to know the state of the medium by sensing the presence of other PLC stations and analyzing the received frames, or by listening to the medium activity thanks to the relative power of the signal from the various stations.

The PCS relies on listening to certain received frames, preamble frames, and priority frames.

The VCS does not actually allow listening to the medium but reserves it by using the PCS.

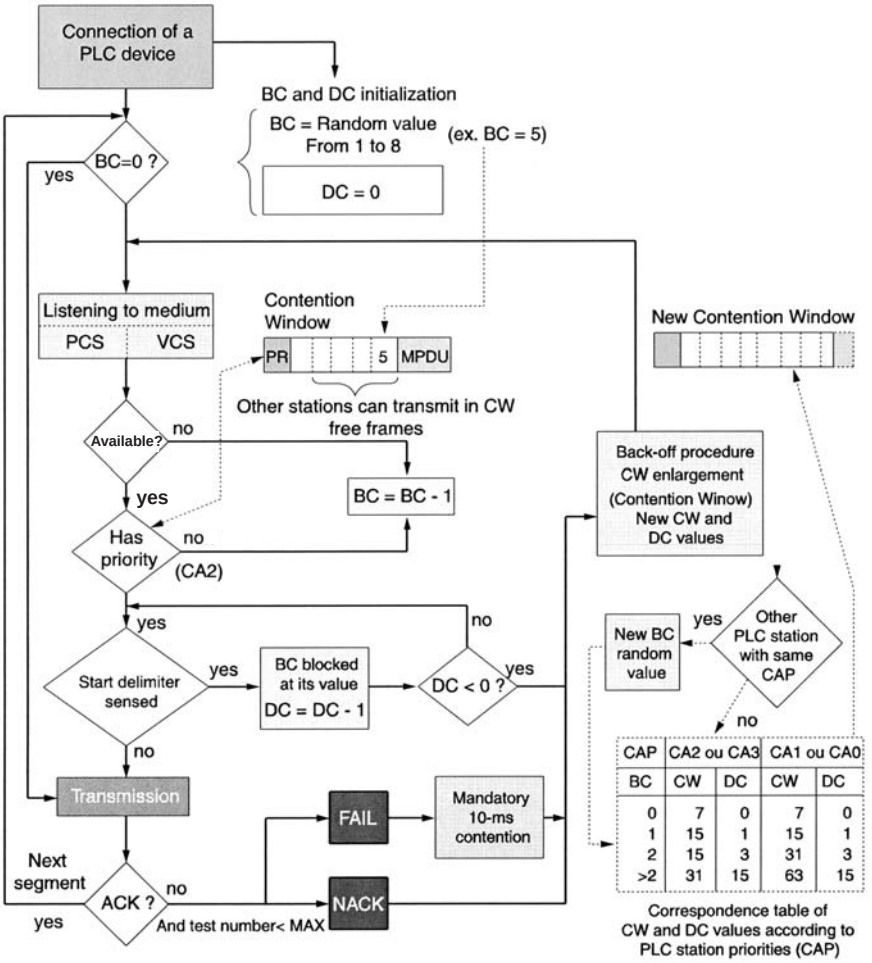

Figure 3.5 CSMA/CA operation in HomePlug 1.0

Two types of mechanisms are used in the VCS:

- detection of fields at the beginning of the frame;
- wait for response information provided by the frame control fields.

Figure 3.6 illustrates these two medium listening techniques before the data frames are transmitted over the electrical network.

Access to the Medium

The access to the medium is controlled using a mechanism called IFS (interframe spacing). This spacing corresponds to the time interval between the transmission of two frames. In fact, the IFS intervals are idle periods on the transmission medium used to manage medium accesses for the stations and to establish a priority system during a transmission.

The values of the various IFSs depend on the physical layer implementation. Three types of IFS are defined by the HomePlug 1.0 standard:

- *CIFS (contention distributed interframe spacing)*. The CIFS is used by stations wishing access to the medium when it is free, leading to the end of other transmissions during 35.84 μs. The CIFS is followed by the priority solving phase for each station.

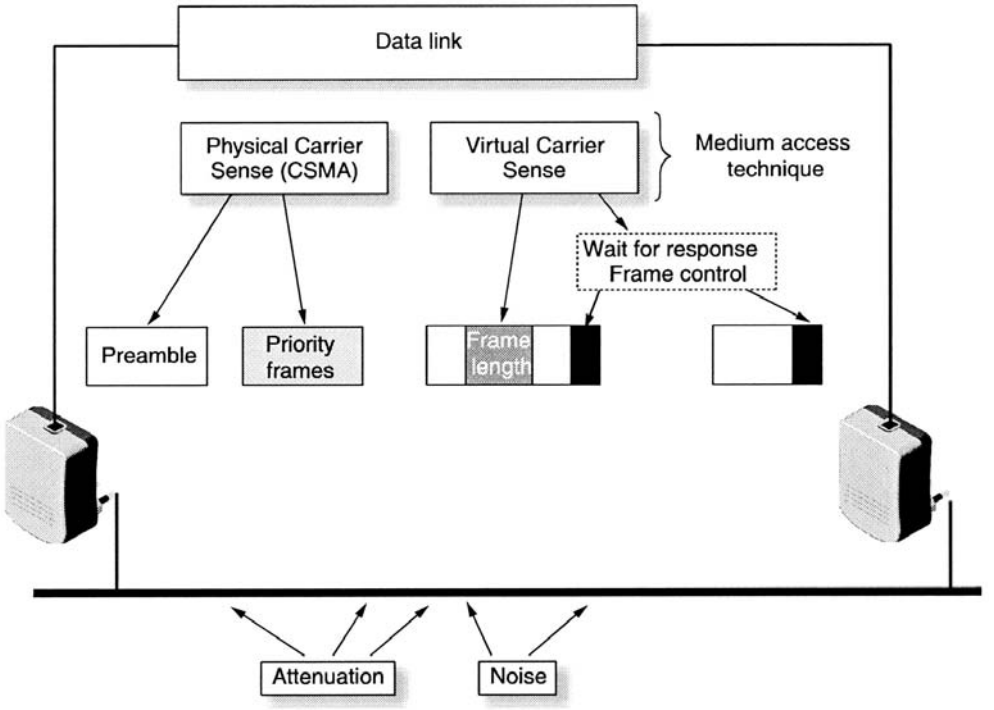

Figure 3.6 Listening to the medium in HomePlug 1.0

- *RIFS (response interframe spacing)*. When a station waits for a response from the destination station, the latter waits for a RIFS time of 26 μs before transmitting its response. This RIFS is also used by the stations to change from sending mode to receiving mode.
- *EIFS (extended interframe spacing)*. The EIFS corresponds to the maximum time that is necessary for a station to transmit. It corresponds to the sum of data frame circulation time in non-ROBO (robust OFDM) mode with its various delimiters, of priority intervals of the CIFS, RIFS, and EFG (End of Frame Gap), which is 1,695 μs. The EIFS time is also used to determine how long the medium is occupied after a collision and for the FEC (forward error control) process, it used to check whether or not there are errors in the received data. The frame length measurement is not determined in a fully robust manner when listening to the medium using the VCS method.

Table 3.4 summarizes the IFS and time slot values of HomePlug 1.0 and HomePlug AV.

The AV version of the HomePlug standard has a number of additional IFS compared with version 1.0.

- *AIFS (allocation interframe spacing)*. Used to separate the TDMA and CSMA/CA allocation areas from the services reserved for the HomePlug AV standard.
- *B2BIFS (beacon to beacon interframe spacing)*. Used to separate the various beacon frames in the specific TDMA allocation area from HomePlug AV beacon frames.
- *BIFS (burst interframe spacing)*. Used to separate the various MPDU frames in the case of the bursting type network mode with access to the CSMA/CA medium.
- *CIFS AV (contention distributed interframe spacing version AV)*. Used by the stations that wish to access the medium in order to separate the transmission

Table 3.4 IFS and Time Slot Values According to the Physical Layer

	Homeplug 1.0	*Homeplug AV*
Time slot	35.84 μs	35.84 μs
CIFS	35.84 μs	100 μs
RIFS	26 μs	30 to 160 μs 140 μs (by default)
EIFS	1,695 μs	2,920 μs
AIFS	—	30 μs
B2BIFS	—	85 μs
BIFS	—	20 μs
CIFS AV	—	100 μs
RGIFS	—	80 μs

frames coming from the source station from the response frames coming from the destination station.

- *RGIFS (reverse grant interframe spacing)*. Used for frame separation in the Reverse Grant network mode specific to the HomePlug AV standard.

Back-off Algorithm

As explained above, the PLC uses the CSMA/CA method to control access to the transmission channel.

Since collisions cannot be detected due to the attenuation and noise on the electrical medium, when a PLC station wants to transmit, it must wait until the medium is available for transmission. The station must wait until an IFS is free for a random period of time, called *back-off* time. As there is no guarantee that a collision will not occur in the meantime, the source (transmitting) station waits for a positive acknowledgment (ACK) frame from the destination station. The destination station transmits a good receipt response if the data is received correctly. This ACK response is transmitted in the next available IFS.

In PLC, the time is sliced into intervals or time slots. These time slots are managed by a timer applied to transmissions and retransmissions of the various stations so that they both have equal probability of accessing the medium.

The back-off algorithm defines a CW (contention window) or back-off window. This parameter corresponds to the number of time slots that can be selected to calculate the back-off timer.

It is between the CW_{min} and CW_{max} values predefined by the HomePlug standard. This time slot number, called BC (back-off counter), is used by the back-off procedure when the medium is busy or when the source station has not received an ACK frame from the destination station. As soon as a station wants to transmit information, it listens to the medium thanks to the PCS defined previously.

If the medium is not busy, it defers its transmission while it waits for an IFS. When the IFS times out, and if the medium is still free, it directly transmits its frame without using the back-off algorithm. Otherwise, since the medium is occupied by another station, the station waits until it is free; it in other words defers its transmission.

To try to access the medium again, it uses the back-off algorithm. If several stations wait for transmission, they all use the back-off algorithm. A station ignores the number of stations associated with the network. Without this mechanism, by which each station potentially calculates a different back-off timer to defer its transmission, the stations would directly collide with each other as soon as the medium is released.

The stations calculate their timer, or $T_{BACKOFF}$, according to the following formula:

$$T_{BACKOFF} = Random(0, CW) \times \text{time slot}$$

$Random(0,CW)$ is a uniform pseudorandom variable within the [0, CW – 1] interval. Therefore, $T_{BACKOFF}$ corresponds to a time slot number. This algorithm randomly extracts various timer values for each station.

Figure 3.7 illustrates the variation of the contention window (*CW*) and of the transmission failure counter (DC) according to the number of retransmissions. These values change from an initial value to a threshold value, which generally indicates an overall problem with the network over which the station wants to transmit.

When the medium becomes free again, and after a CIFS and frame prioritization phase, the stations make sure that the medium is still free. If this is the case, they decrement their timer's time slot by time slot until the timer of a station times out. If the medium is still free, this station transmits its data by prohibiting access to the medium to the other stations that block their timers.

The back-off procedure can be used even when no collision occurs. A station increments its BPC (back-off procedure counter) as soon as a collision is detected or when the BPC reaches zero. During the back-off, if another station transmits first, the station checks it's DC (deferral counter) and decrements it until it reaches zero. After having decremented its DC, a station blocks its timer at the BPC value.

Once the station transmission is complete, the other stations still wait during a CIFS and the priority phase. They check whether the medium is occupied during and after the CIFS, then decrement their timers again where they had blocked this timer until another station transmits data. However, they do not extract a new timer value. Since they have already waited for medium access, they are more likely to have access to it than stations just starting their attempts.

If the DC reaches zero, all the stations waiting for transmission must go through a back-off procedure and defer the transmission of their data.

When calculating the timer, two or more stations may extract the same timer value, which therefore times out at the same time, resulting in a simultaneous transmission over the medium and causing a collision. After the back-off procedure, the stations therefore reset the back-off algorithm for a new transmission if necessary by obtaining a new *CW* and DC value. If a station receives a good receipt frame (ACK), these values are reset to their minimum value.

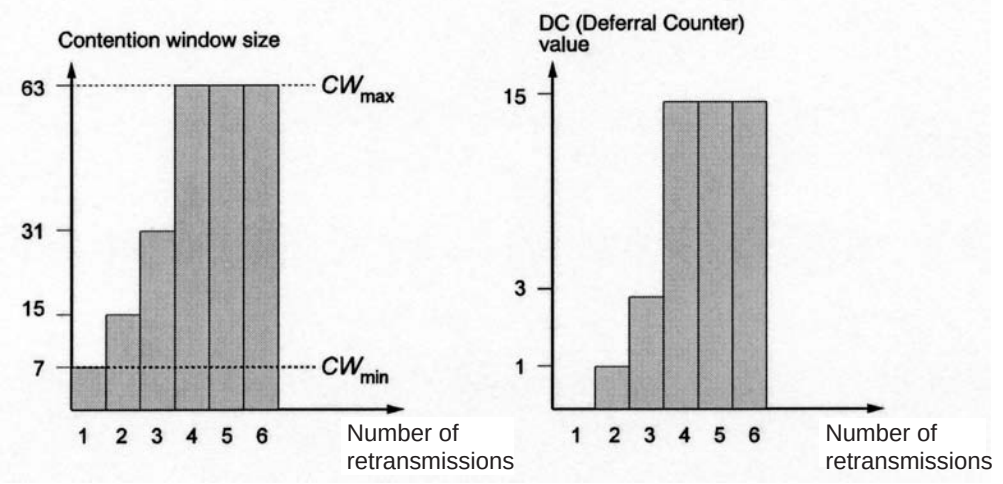

Figure 3.7 Contention window size variation according to the back-off algorithm

If *CW* and DC reach their maximum value defined by the HomePlug 1.0 standard, these values are maintained, even if the BPC is decremented.

As explained above, when the algorithm is used, the stations of the same network have the same probability of accessing the medium. The only drawback with this algorithm is that it doesn't guarantee a minimum time. Therefore, it is difficult to use within real-time applications such as voice or video.

TDMA and Medium Access in HomePlug AV

Since the CSMA/CA algorithm does not guarantee a minimum transmission time, the HomePlug AV standard, a HomePlug 1.0 extension, implements an allocation of transmission time slots based on the TDMA (time division multiple access) medium access system.

This medium access system is used for a deterministic allocation of the transmission times for each station. This allocation is managed by the CCo device, which coordinates the various network stations' access to the medium.

Figure 3.8 illustrates the time division of the time spaces in the TDMA multiplexing technique. We notice that the time base of a transmitted frame is divided into TDMA blocks corresponding to time spaces dedicated to communications between two stations. During the TDMA1 block, for example, only stations 1 and 2 communicate between themselves. This ensures the time organization of the communication over the PLC network.

Therefore, HomePlug AV specifies determined time periods corresponding to two periods of the 220 V/50 Hz electrical signal synchronized on signal zero crossings. These TDMA time areas are divided into several determined and fixed time allocations. One of the time allocations is reserved for CSMA/CA frames and frame exchanges complying with the HomePlug 1.0 and HomePlug AV standards.

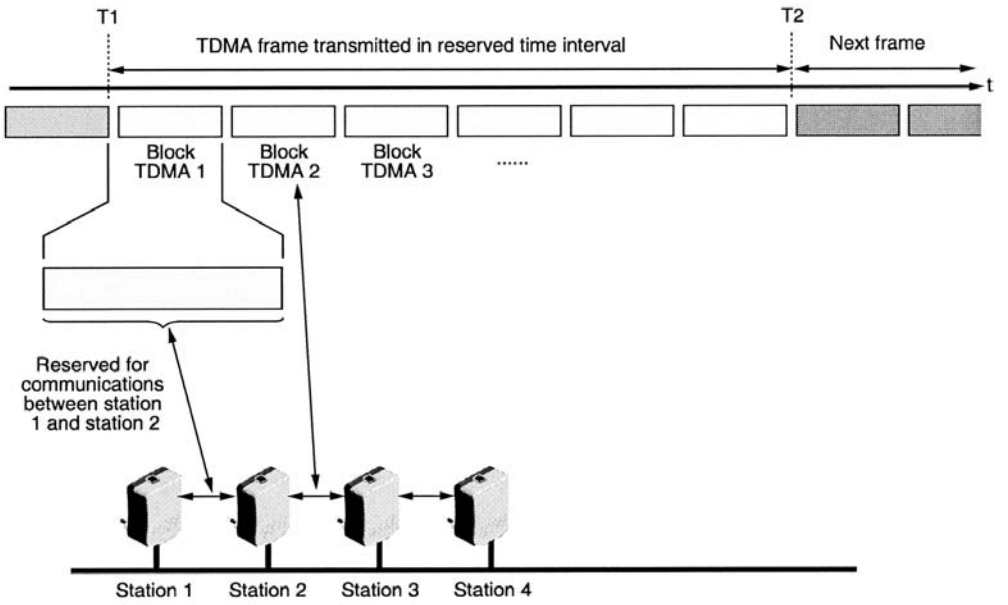

Figure 3.8 Time division of TDMA time spaces for a PLC frame

Data Transmission Example

When a source station wants to transmit data to a destination station, it makes sure that the medium is not busy. If no activity is sensed during a time period corresponding to a CIFS, the source station waits for the prioritization period then transmits its data.

Figure 3.9 illustrates the role of the timers during the transmission of a data frame and its acknowledgment.

If the medium is busy, the station waits until it is free. Once the medium is free, the station waits during a CIFS then, after having checked that the medium is free, initiates the back-off algorithm to defer once again its transmission in order to avoid any collision. When the timer of the back-off algorithm times out, and if the medium is free, the source station transmits its data to the destination station.

When two stations or more have simultaneous access to the medium, a collision occurs. In this case, these stations reuse the back-off algorithm to have access to the medium. If the sent data is received correctly—to know this, the destination station checks the data frame CRC—the station involved waits during an RIFS time interval and sends an ACK to confirm the correct receipt.

If this ACK is not sensed by the source station, if the data is not received correctly, or if the ACK is not received correctly, a collision has supposedly occurred and the retransmission procedure is initiated.

The ARQ (Automatic Repeat Request) Process

When a source station transmits its data over the medium, it waits for an acknowledgment frame from the destination station. This frame is potentially followed by a procedure for the retransmission of non-received or erroneous data called ARQ (automatic repeat request).

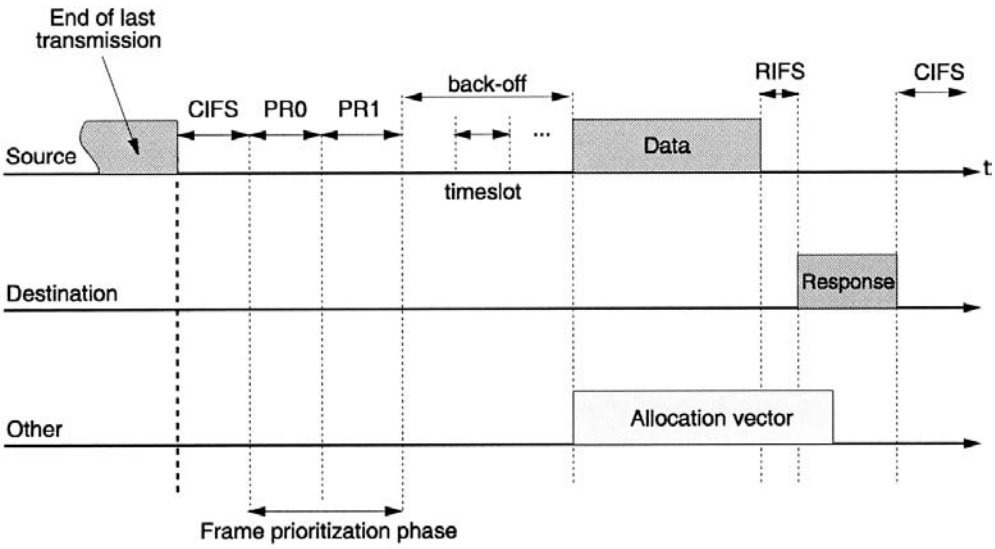

Figure 3.9 Role of the timers in data transmission

The destination station can resend three types of acknowledgment frames:

- *ACK*. The destination station has correctly received the data contained in the frames and this data is correct.
- *NACK*. The destination station has correctly received the data but some data is damaged. This check is carried out using the CRC (cyclic redundancy check) value. The destination station then asks the source station to resend the damaged data segment.
- *FAIL*. The data has not reached the destination station or the station buffer is full and cannot receive and process the data.

Figure 3.10 illustrates, in terms of time, the various acknowledgment response types in the HomePlug 1.0 PLC standard. This process improves the medium access quality by allowing exchanges between the source stations and the destination stations.

The source and destination stations use one of the fields present in the data frame to determine the response frame that will be resent to the source station. This field, which is called FCS (frame check sequence), is used to check the integrity of the data received by the destination station.

In the same way, the destination station resends the acknowledgment with a part of this field, the RFCS (response FCS) field. This field is used by the source station to know whether the data has been correctly received by comparing the transmitted FCS with the received RFCS (see Figure 3.11).

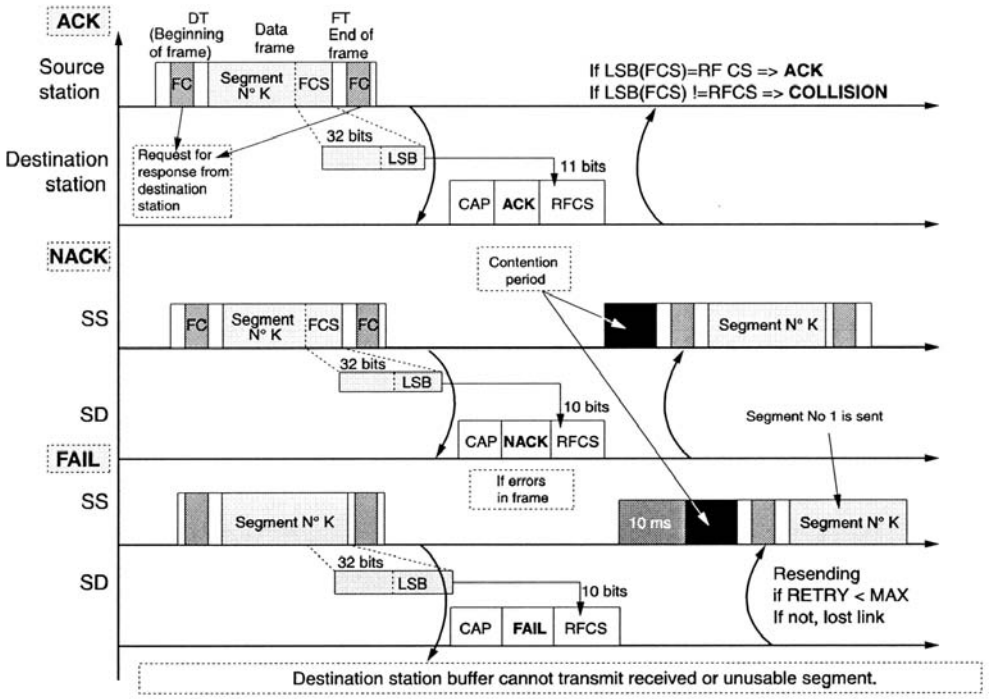

Figure 3.10 Acknowledgment frames in the ARQ process

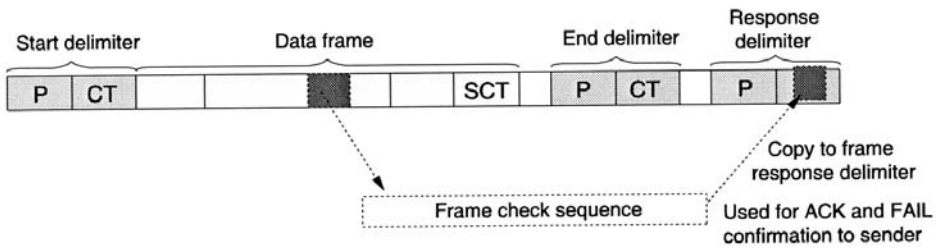

Figure 3.11 Frame check using the FCS and RFCS fields in the ARQ process

ACK Response

In the case of an ACK acknowledgment by the source station, the destination station resends to it a response frame containing the RFCS field of the data frame transmitted by the source station. This field is used by the station to know whether the data has been correctly received by the destination station or whether a collision that may have caused a corruption of the data transmitted over the medium occurred.

Figure 3.12 illustrates this acknowledgment mechanism in the HomePlug 1.0 standard.

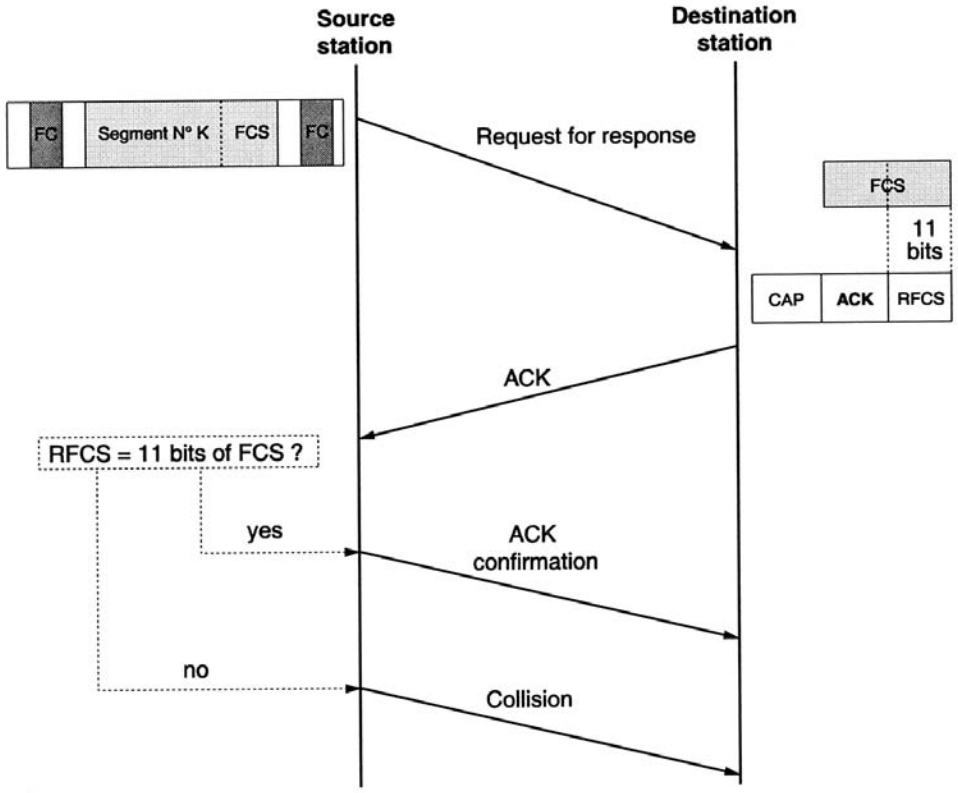

Figure 3.12 ACK type acknowledgment in HomePlug 1.0

NACK Response

In the case a NACK type acknowledgment, the destination station resends to the source station a response frame after a contention period in order to indicate that the data has been damaged during the transmission. The source station resends in its turn to the destination station a confirmation of the NACK acknowledgment and retransmits the damaged data frame segment (see Figure 3.13).

FAIL Response

The FAIL response indicates that the destination station could not use the received data frame due to a collision or a congestion of the data receipt buffer. The destination station cannot foresee the data rate that it will receive and can be incapable of storing all the received data.

A 10-ms contention period specific to FAIL responses is mandatory in this case (see Figure 3.14).

The destination station records the number of times that the FAIL status has appeared in the segment. If this number exceeds a given threshold, the destination station asks the source station to resend the service block from the first segment.

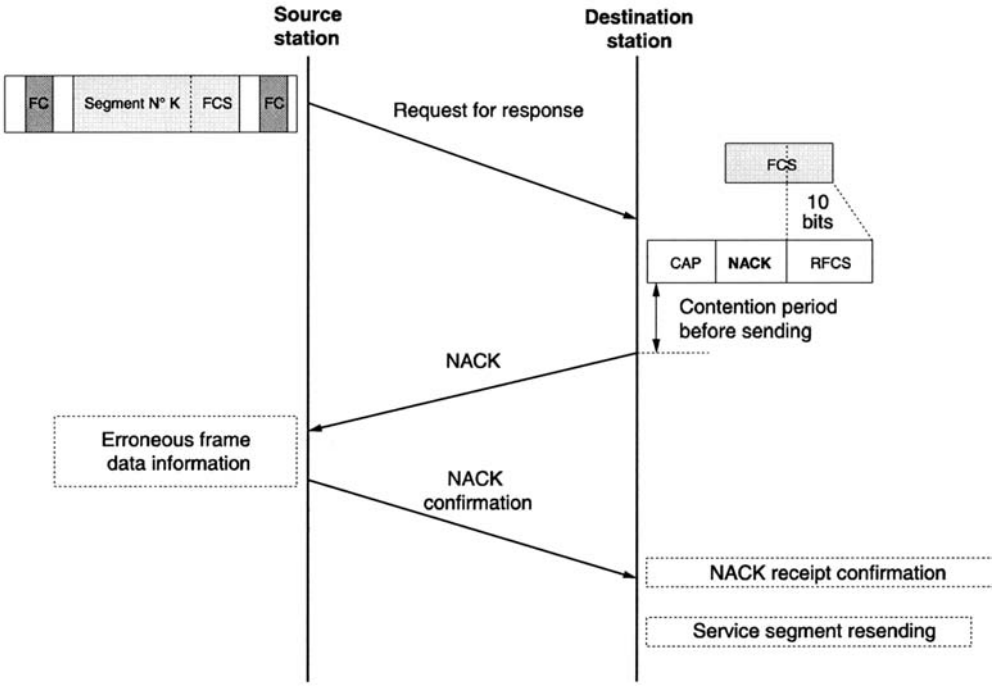

Figure 3.13 NACK-type acknowledgment in HomePlug 1.0

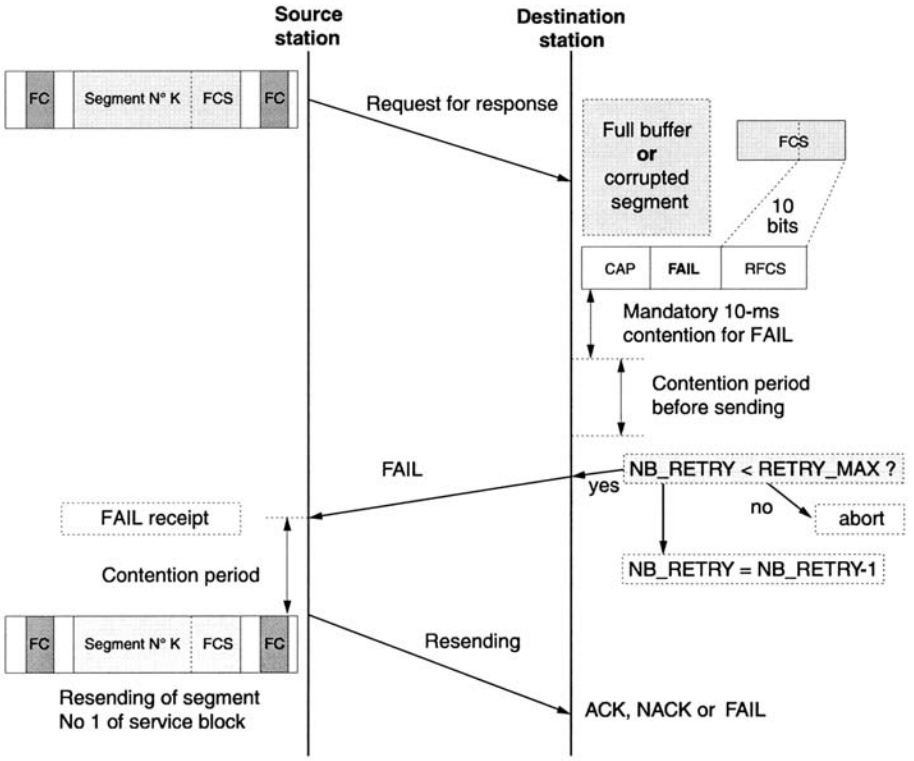

Figure 3.14 FAIL response in HomePlug 1.0

SACK Response in HomePlug AV

In the AV version of the HomePlug standard, an additional response, the SACK (Selective ACK) response, has been added to compensate for the fact that the PLC links between two stations are not necessarily symmetrical in terms of useful throughput. Due to the characteristics of the electrical network, the data transmissions are not under the same influences in one direction as in the other one. The SACK response is used by the central device of the PLC network, the CCo, to manage global links, i.e., the various links between PLC stations of the network, and the transmission time allocations within the framework of the TDMA medium access technique.

Synchronization and Frame Controls

The frames are checked using the FCS field that is included in the data block of the frame. This field is used by the destination station to resend the suitable response type (ACK, NACK, or FAIL) to the source station.

The source station then checks the integrity of this response using the RFCS field of the response frame, as illustrated in Figure 3.15.

The response frame is sent by the destination station after an interframe period of 26 μs minimum and 1,695 μs maximum (see Figure 3.16). Since the defined size of the response frame is much shorter than the data frames, it is much more likely to be transmitted and does not occupy much of the total bandwidth.

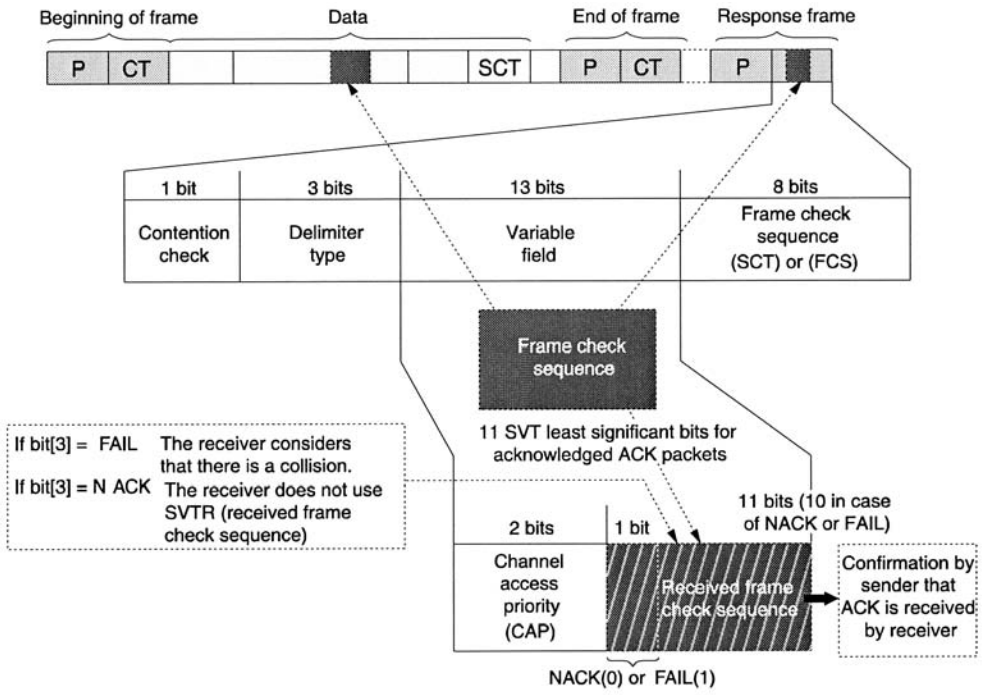

Figure 3.15 Frame check sequence (FCS)

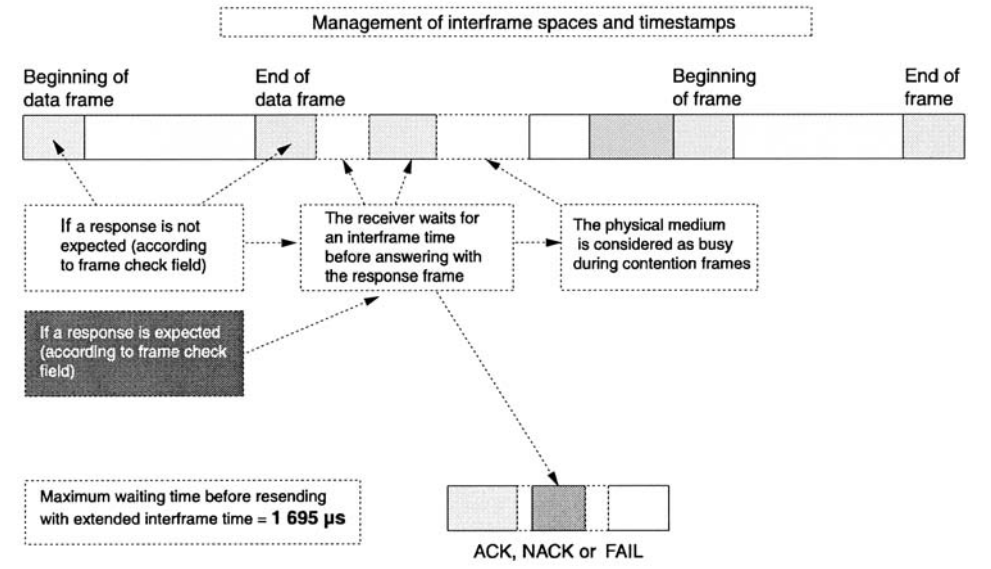
Management of interframe spaces and timestamps
Beginning of data frame
End of data frame
Beginning of frame
End of frame
If a response is not expected (according to frame check field)
The receiver waits for an interframe time before answering with the response frame
The physical medium is considered as busy during contention frames
If a response is expected (according to frame check field)
Maximum waiting time before resending with extended interframe time = 1 695 µs
ACK, NACK or FAIL

Figure 3.16 Management of interframe spaces

Synchronization of HomePlug AV Frames

Recent PLC developments made it possible to improve the performance of the devices while keeping the interoperability with the devices of previous versions. Within the HomePlug consortium, the latest developments made it possible to pub-

lish the specifications of the HomePlug AV (for Audio and Video) version which is much more efficient for the management of the quality of service (QoS).

Figure 3.17 illustrates the organization of the beacon frames in HomePlug AV. This standard, based on a master-slave architecture, uses CSMA and TDMA medium access functionalities. CSMA is preferred for data traffic with a medium or no priority level and TDMA for data traffic with priority, for which the QoS is important (real-time data flow, like in VoIP, or high data flows, like in VoD).

The QoS management is obtained by means of a very efficient technique specific to PLC technologies that consists of synchronizing TDMA beacon frames on the 50 or 60 Hz signal of the electrical network. This fully deterministic signal is synchronized over the entire public electrical network and private electrical networks. Therefore, the PLC devices can be synchronized without a specific clock by using 50 or 60 Hz signal zero crossings.

This technique makes it possible to obtain the efficient determinisms that critical data communications require. The master of the PLC network manages the allocations for access to the TDMA slots between the slave devices of the network according to their requirements.

Managing Frame Priorities

The frame priority for medium access is managed by the CAP (channel access priority) field and the size of the contention window (CW), as illustrated in Figure 3.18.

The CAP variable affects the medium access as we have seen in Figure 3.7, where the CW and DC parameters are set by the back-off procedure and given by the correspondence table according to the respective CAP values of the network PLC devices.

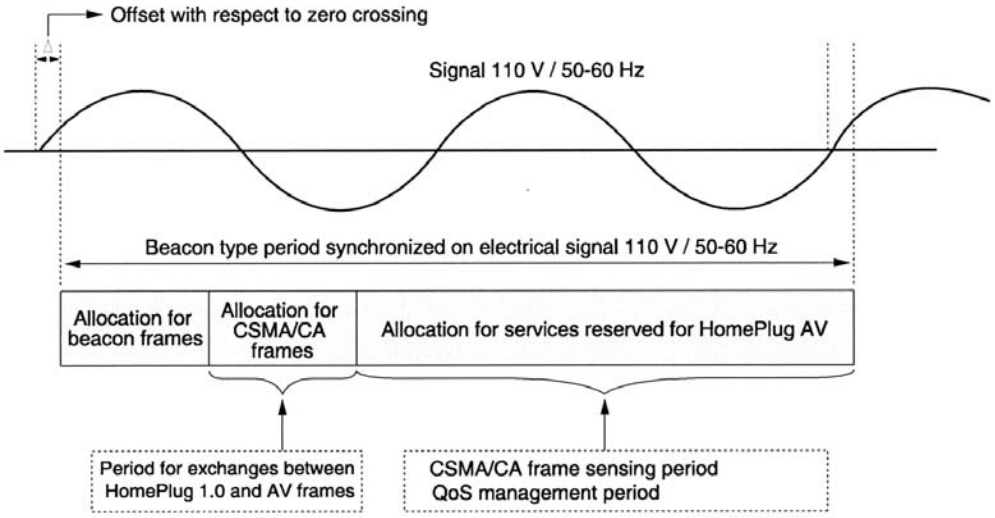
Offset with respect to zero crossing
Signal 110 V / 50-60 Hz
Beacon type period synchronized on electrical signal 110 V / 50-60 Hz
Allocation for beacon frames
Allocation for CSMA/CA frames
Allocation for services reserved for HomePlug AV
Period for exchanges between HomePlug 1.0 and AV frames
CSMA/CA frame sensing period
QoS management period

Figure 3.17 Synchronization of HomePlug AV beacon frames on the 50 Hz signal

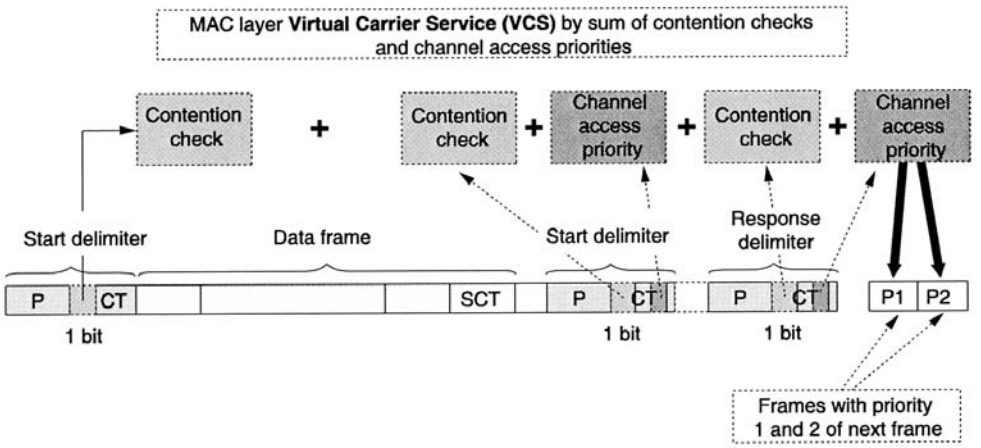

Figure 3.18 Frame priority management by the CAP (channel access priority) variable

The CAP variable is used by a PLC station to inform the other stations of its medium access priority. This variable determines the values of the PRP1 and PRP2 priority frame data that is read by the network PLC stations to determine the various priority levels. Therefore, the other stations are informed in advance of the priority of each of the PLC devices.

This entire process, called VCS (virtual carrier sense), is used in conjunction with PCS (physical carrier sense) during medium access attempts.

Managing Frequency Channels (Tone Map)

As we have seen before, there are several OFDM symbol modulation techniques according to the quality of the PLC links between the devices. Unlike Wi-Fi, where each station can configure the frequency channel over which it wishes to transmit data, in PLC, the entire frequency band is used.

Figure 3.19 illustrates a simple network with four PLC stations. Each of them assesses the quality of the PLC link connecting it to the other stations. It then stores this information in the correspondence table of a register of the PLC device. This register can be accessed using one of the beginning frame delimiter fields called a tone map. Each station regularly updates the tone map table; the updating time may vary from 10 ms to several seconds according to the PLC station parameterization.

It may happen that some stations see each other at the PLC level whereas other stations do not see each other. It is important that the stations used as a gateway to other networks see all the stations involved by the other network. For example, in the case of Figure 3.19, PLC1 cannot have access to the Internet since, though the links to PLC2 and PLC3 are correct, the transmission channel cannot be used towards PLC4. If the electrical wiring is too long or if the electrical network is too disturbed, this results in an attenuation and a degradation of the PLC signal making upper layer data communications impossible.

Figure 3.20 illustrates all the fields of the start delimiter. In the variable field, the first five bits are used by the tone map table. This tone map is used to store the status of the links toward fifteen other PLC stations. This determines the limit relating to

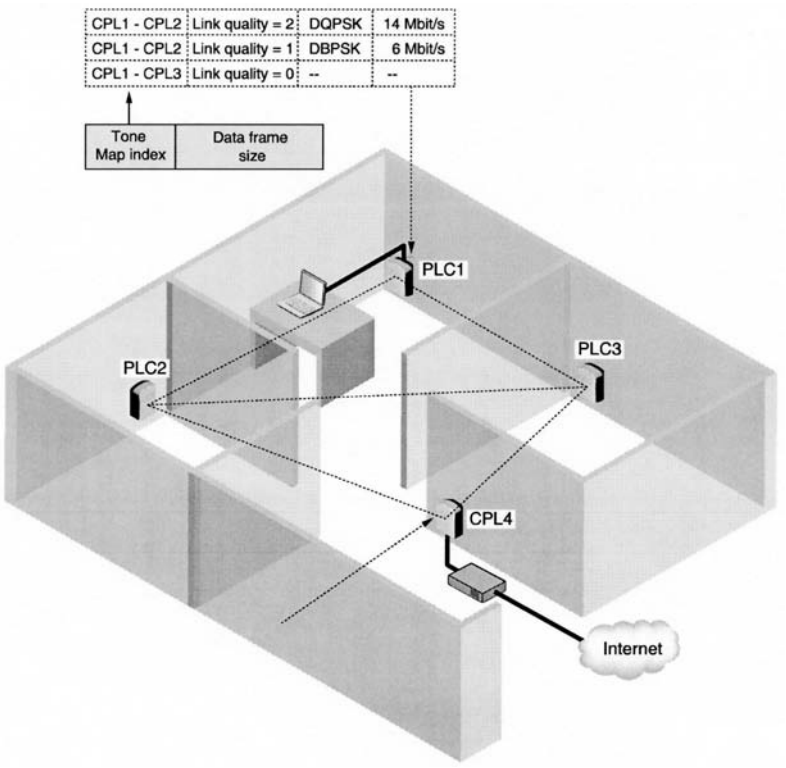
CPL1 - CPL2 Link quality = 2 DQPSK 14 Mbit/s
CPL1 - CPL2 Link quality = 1 DBPSK 6 Mbit/s
CPL1 - CPL3 Link quality = 0 -- --
Tone Map index
Data frame size
PLC1
PLC2
PLC3
CPL4
Internet

Figure 3.19 Tone map management between PLC devices

the number of possible PLC stations in the same PLC network (16 stations for HomePlug 1.0 and 1.1 and 250 stations in HomePlug AV). Some values are reserved for the ROBO mode or for particular implementations of the HomePlug 1.0 standard.

Segment Bursting and Contention-Free Access

Two particular modes, segment bursting and contention-free access, are used to have access to a higher priority on the PLC network in order to send the successive segments of a service block without waiting for mandatory contention windows before transmitting the frames.

In the case of segment bursting, PLC stations with priority level CA3 can set the CC (Contention Control) parameter to 1. It is then possible for the source station to transmit two consecutive segments without waiting for a high contention value. This mode improves the performance and can prove useful for applications of the VoIP type demanding a particular priority exception.

Figure 3.21 illustrates the functionality of segment bursting, which makes it possible for a PLC device to transmit a series of service blocks with maximum priority (CA3).

In the case of contention free access (CFA), the source station is allowed to send all the segments with priority CA3 and to transmit seven consecutive MPDU by setting the CC field to 1.

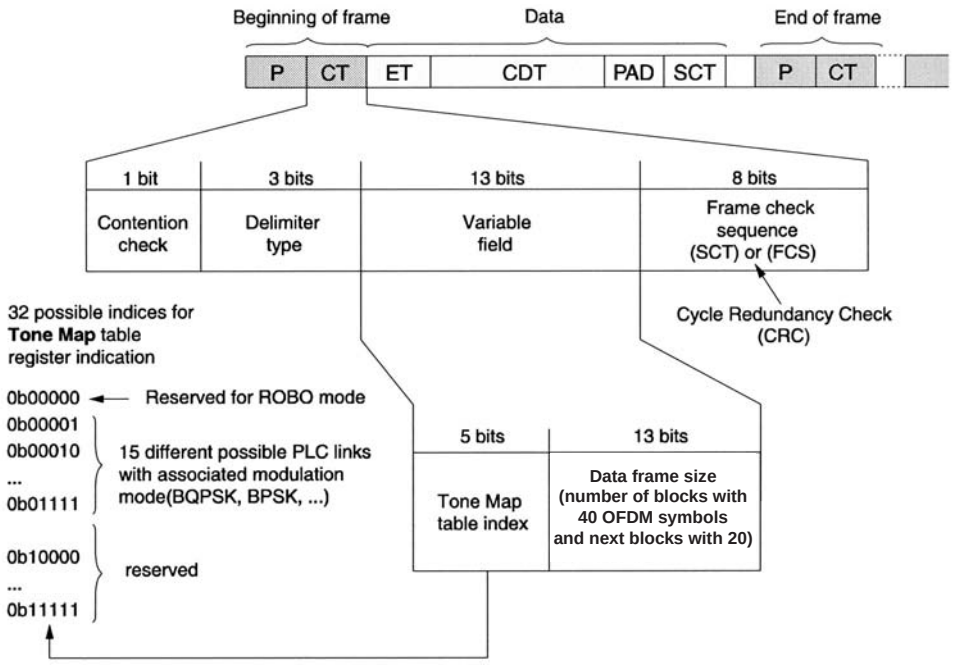

Figure 3.20 HomePlug 1.0 start delimiter details and associated tone map

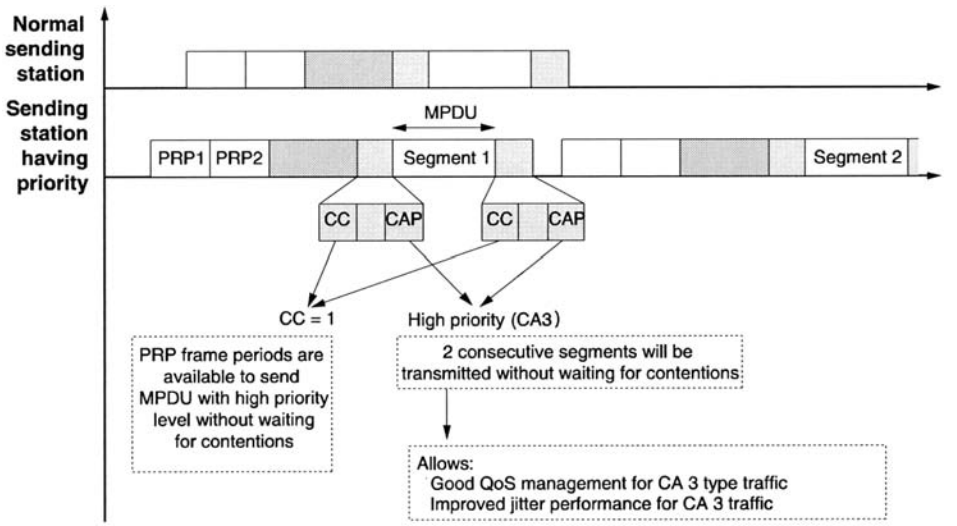

Figure 3.21 Segment bursting mode management

Frame Level Functionalities

It is important to remind the structure of the data frames transported over the electrical network in order to understand the network functionalities of the PLC technologies.

The network modeling into seven layers according to the OSI model makes it possible to understand how the PLC technologies structure data exchanges for each protocol layer. The PLC technologies come into play at the PHY and MAC layer levels only. Because of this, they are considered as IEEE 802.3 Ethernet networks from their interfaces. Therefore, the network engineers only have to consider the IP, TCP, and application configurations seen by the user of PLC technologies.

Figure 3.22 illustrates the place of PLC technologies with regard to the layers of the OSI model.

MAC Encapsulation

Unlike IEEE 802.11 frames, on which the protocol layers of the Wi-Fi technologies are based, the PLC frames can be considered as MAC encapsulations.

Figure 3.23 illustrates the MAC encapsulation of HomePlug 1.0 PLC frames.

From the point of view of the data link layer, the MAC Ethernet frames are de-encapsulated from the physical frames for their presentation to the Ethernet interface of the PLC devices.

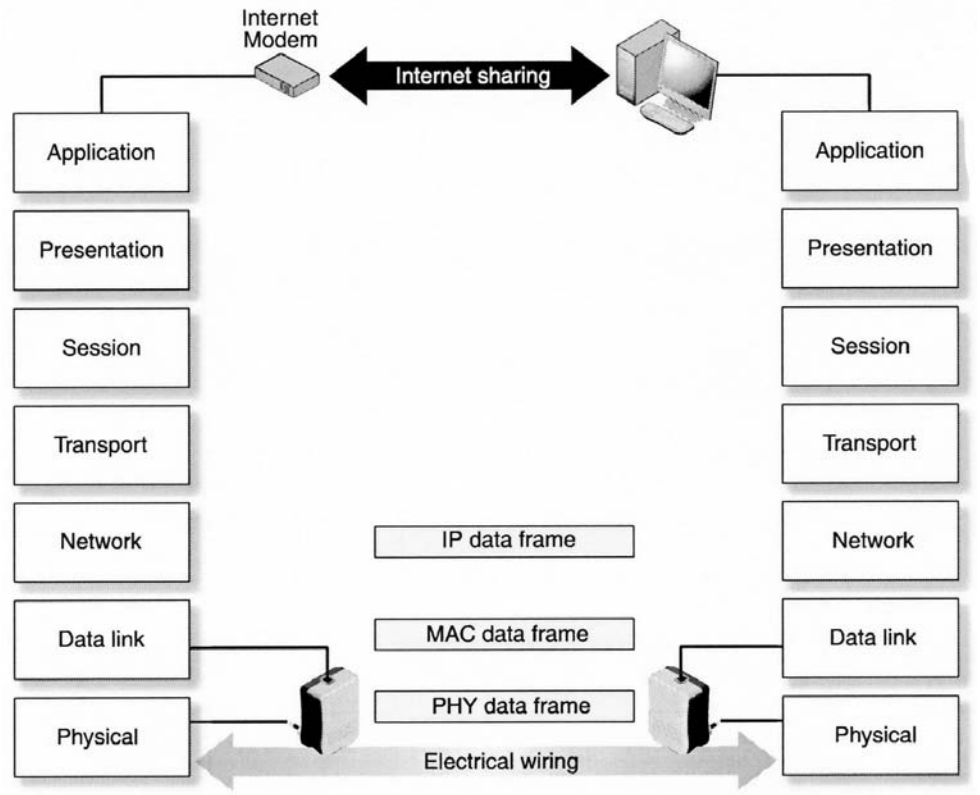

Figure 3.22 PLC technologies and the OSI model

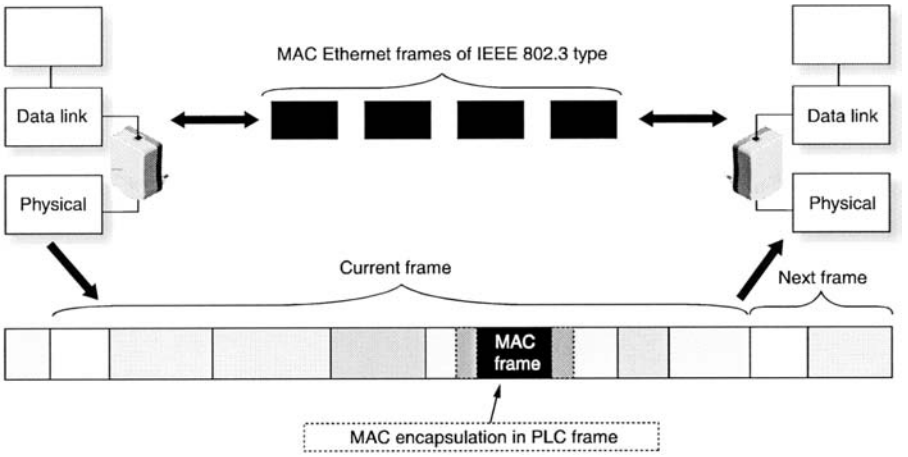

Figure 3.23 MAC encapsulation in HomePlug 1.0

Fragmentation Reassembly

In a PLC transmission using a shared medium disturbed by other uses with a wired Ethernet link using a cable dedicated to data communications, the error rate for the electrical wiring is higher (10^{-5} for the electrical wiring against 10^{-9} for the Ethernet cable).

The PLC link may be subjected to various constraints, such as attenuation due to interference, multipath over the electrical wiring, or electrical wiring crosstalk effects. These constraints result in the attenuation of the signal power, which no longer makes it possible for the PLC link to deliver data correctly.

A high error rate results in the retransmission of all the erroneous data sent over the network. This retransmission entails a high cost in terms of use of the bandwidth, especially when the size of the data sent is high.

To avoid wasting the bandwidth to a large extent, a fragmentation mechanism is used; it reduces the number of retransmissions in environments with a high noise level like PLC.

Fragmentation

The data frames of the network layers (IP, and so forth) or of upper layers are seen by the data link layer as successive MPDUs (Mac Protocol Data Unit) forming SB (service blocks). The SB are then sliced into segments with 1,500 bytes maximum.

Therefore, the size of a segment can be 1,500 bytes or less. In the latter case, it is filled with padding bits in order to obtain a MPDU with a fixed size. The 1,500 byte size corresponds to 160 OFDM symbols for the physical layer.

Each of the segments forming the SB is numbered for its recognition; this makes it possible to reconstitute the SB sent by the source station (source address at MAC level) to the destination station (destination address).

Figure 3.24 illustrates the various segments sent by the source station and numbered for their identification by the destination station. As we shall see with the ARQ functionalities of the MAC layer, if one of the SB segments is not received by

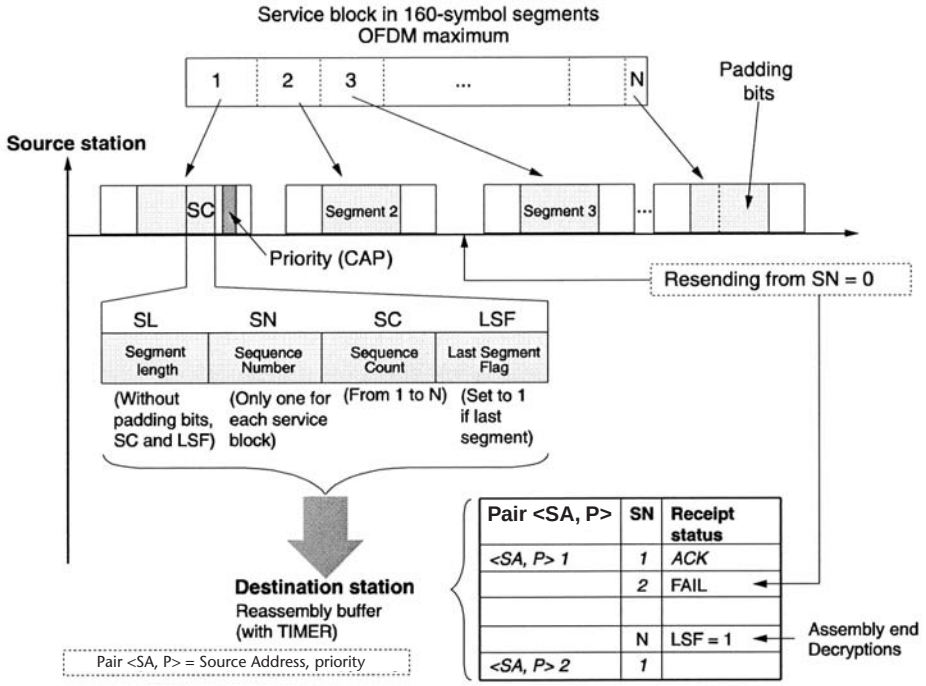

Figure 3.24 Data frame fragmentation

the destination station or is damaged when it is received, NACK (non-acknowledgment) or FAIL (failure) processes are implemented between the source station and the destination station prior to the resending of the missing or damaged segments.

Reassembly

When they are received, the segments are buffered and indexed in the reassembly buffer of the destination station with the station address and priority. Once all the segments of a SB are received, the data block is de-encapsulated and transmitted to the OSI model upper layers. The SB then form IP frames with TCP or UDP headers.

The reassembly buffer can then be emptied so that the next frames can be received. The size of the buffer is intended to favor the maximum transmission speed over the transmission channel. However, since access to the medium (CSMA) is not deterministic, the buffer cannot anticipate the segment transmission speed and can find itself in a saturation situation, in which it can no longer accept additional segments. It then asks the source station to resend the segments that are not processed at a later time.

Other Functionalities

The PLC implement other network functionalities in order to optimize the use of the transmission channel, in particular in terms of data transmission speed.

This is achieved with the dynamic adaptation of the data rate at the physical level according to the quality of the PLC links.

Optimum use of the global bandwidth can also be made by sending the data only to the PLC devices involved. These functionalities correspond to those found in other network technologies, such as Wi-Fi.

Dynamic Adaptation of the Bit Rate

As indicated before, the PLC technology permanently readjusts the condition of the links between network stations.

Since the PLC links depend on the medium condition and interference with the other electrical devices connected to the network or inductive, the transmission speed must be permanently readjusted by choosing the modulation mode for OFDM symbols forming the frames.

For the user, the useful bit rate between the terminals connected to the PLC network dynamically varies according to the PLC links.

Table 3.5 lists the various transmission speeds or PHY bit rate of the PLC devices of the HomePlug 1.0 standard according to the tone map determined for each station with regard to the other stations of the network.

Unicast, Broadcast, and Multicast

Insofar as the PLC can be seen as MAC encapsulation techniques, the various modes for MAC frame sending, whether these are unicast, broadcast, or multicast modes, are authorized.

In the unicast mode, a network station transmits data to a single other station using its MAC address. In broadcast mode, on the contrary, a station transmits its data to all the stations of the network using a MAC address dedicated to this mode and with all the bits to 1. In multicast mode, a station transmits to a group of other network stations using a single MAC address for the entire station group. For this purpose, the station group with the associated MAC addresses must have been predefined. A prefix is used by the multicast MAC addresses for their recognition on the network. This prefix uses the first twenty-four bits (out of 48) of the MAC address.

As we'll see in Chapter 5, the broadcast and multicast modes are supported using the multicast flag (on one bit) of the block control field of the MPDU data frame.

Table 3.5 Dynamic Bit Rates of the HomePlug 1.0 Standard

MODULATION TECHNIQUE	*ENCODER PARAMETER*	*FEC (CODING RATE OF CONVOLUTIONAL CODE*	*PHY BIT RATE (Mbit/s)*	
DQPSK	23/39 to 238/254	¾	14.1	139 possible PHY bit rates between 0.9 and 14
DQPSK	23/39 to 238/254	½	9.1	
DBPSK	23/39 to 238/254	¾	4.5	
ROBO (DBPSK)	31/39 to 43/51	½	0.9	

The unicast mode is also possible: since the PLC stations are identified by their MAC address, if a station knows the MAC address of another station, it can address the MPDU directly and solely to this station.

Service Quality

The quality of service, which has become very important in IP networks, is used to differentiate the priorities of the various traffic over the network. As we'll see in Chapter 6, the IP services require different constraints in terms of transmission speed, network travel time, and jitter between the frames transmitted over the network.

These constraints are decisive for applications and for the upper layers of the OSI model to maintain a TCP connection for HTTPS traffic, an FTP connection, and so forth.

Therefore, it is necessary to implement priority levels for MAC level and physical level frames according to the constraints of the upper layer applications. This must be done in the frames insofar as the medium is shared as a MAC level network hub.

The quality of service is made possible in PLC networks with the priorities of the network devices. These priorities are indicated by the CAP parameter, which is interpreted during the priority (PRP1 and PRP2) resolution periods just before the contention frames.

Figure 3.25 illustrates the priority levels (CA0, CA1, CA2, and CA3) in the PRP1 and PRP2 priority resolution periods. The contention bit included in the end

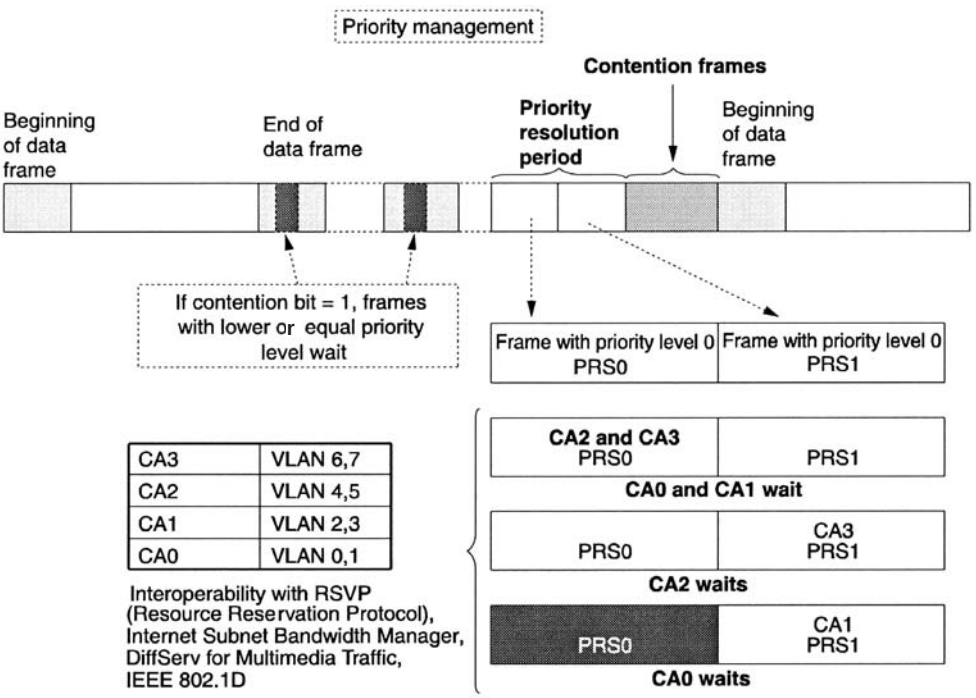
Priority management
Contention frames
Beginning of data frame
End of data frame
Priority resolution period
Beginning of data frame
If contention bit = 1, frames with lower or equal priority level wait
Frame with priority level 0 PRS0
Frame with priority level 0 PRS1
CA3 VLAN 6,7
CA2 VLAN 4,5
CA1 VLAN 2,3
CA0 VLAN 0,1
Interoperability with RSVP (Resource Reservation Protocol), Internet Subnet Bandwidth Manager, DiffServ for Multimedia Traffic, IEEE 802.1D
CA2 and CA3 PRS0
PRS1
CA0 and CA1 wait
PRS0
CA3 PRS1
CA2 waits
PRS0
CA1 PRS1
CA0 waits

Figure 3.25 Quality of service management

delimiter and response frames is used to prioritize the frames with respect to those of the stations with the same priority level or a lower priority level.

Using VLAN Labels

The use of VLAN labels is compatible with PLC technologies, since the value of these labels is interpreted in the value of the PLC station CAP parameter.

One of the advantages of PLC technologies is to allow the creation of virtual networks at several OSI layer levels (PLC virtual networks, VLAN networks, overlay MAC layers, and so forth) providing high flexibility to PLC network integrators.

VLAN labels allow the implementation of a number of IP services for various data traffic and application levels, particularly the following:

- RSVP (reservation protocol);
- Internet Subnet Bandwidth Manager;
- DiffServ for Multimedia Traffic;
- IEEE 802.1D.

CHAPTER 4

Security

Security has been the main problem for Wi-Fi networks. In the case of PLC, this is not so much of a concern as it is difficult to have access to the physical medium. In Wi-Fi, as the transmission medium used is radio, anyone in the network coverage area can intercept its traffic or even reconfigure the network at will. Although the PLC electrical wiring is also a medium shared by the various network devices, it is much more difficult to have access to it and it involves major dangers due to the presence of the 110-220 V/50-60 Hz signal.

However, since the electrical network has a universal extension, the wiring propagates the PLC signal outside the limits of the private electrical network in a conducted or radiated way, which implies the implementation of suitable software security levels.

Current PLC networks can be secured in the same manner as high bit rate wired fixed networks. Any threat can be eliminated by adding authentication servers or secured tunnels, for example.

Security is a major issue for the deployment of local area networks in companies, where the development of IP telephony applications is sustained. In such a background, it is essential to have reliable security mechanisms to avoid any unauthorized listening to communications.

Overview of Network Security Issues

As with any other network, PLC can be subjected to various types of attacks either to interfere with PLC operation or to intercept the transmitted information. However, the advantage of PLC networks comes from the medium they use — the electrical wiring, which makes them particularly resistant to attacks since they are not easily accessible. To avoid any information disclosure, the network traffic must be encrypted in such a way that anyone not belonging to a PLC logical network cannot recover and decipher it.

In addition to eavesdropping, the main attacks to which a network can be subjected are those that aim at preventing its operation until it collapses or at having access to it and reconfiguring it as wished.

The only counterattacks in response to these types of attacks are cryptography, which prevents intruders from having access to data exchanged over the network; authentication, which allows the identification and authorization of anybody wishing

to send data; and integrity control, which is used to know whether the data sent was not modified during the transmission.

Cryptography

Making a text or message incomprehensible through the use of an algorithm is not new. The Egyptians, like the Romans, employed methods used to encode a text or a message. These techniques, which were relatively simple originally, have changed, and cryptography has been recognized as a science since World War II.

The basic principle of cryptography is illustrated in Figure 4.1. An encryption key is used to encode a plain text. The cryptogram is then sent to the recipient. The recipient uses a deciphering key in order to reconstitute the plain text. At any time during the transmission, somebody can recover the encrypted text, called a cryptogram, and try to decipher it using various methods.

Cryptology

Cryptography only involves encryption design and methods. Trying to decipher encrypted text is called cryptanalysis. Cryptology designates the study of cryptography and cryptanalysis.

In France, for example, there are strict regulations concerning the length of the keys used for encryption purposes. A key with a maximum length of 40 bits can be used for any public or private use. For private use, the length of the key may not exceed 128 bits. For a key length exceeding 128 bits, the key must be transmitted to the local cyber security authorities. In the USA or in Japan, the regulations are different and one should take care to know the restrictions on the length of keys authorized to be used.

There are two cryptography techniques: symmetric-key cryptography and asymmetric-key cryptography, better known as public-key cryptography.

Symmetric-Key Cryptography

Symmetric-key cryptography is based on the use of a single key used to encrypt and unscramble data. All persons wishing to transmit data securely must therefore share the same secret: the key. This process is illustrated in Figure 4.2.

The clear fault in this system resides in how this secret key is shared and transmitted between the sender and the receiver.

Figure 4.1 Data encryption

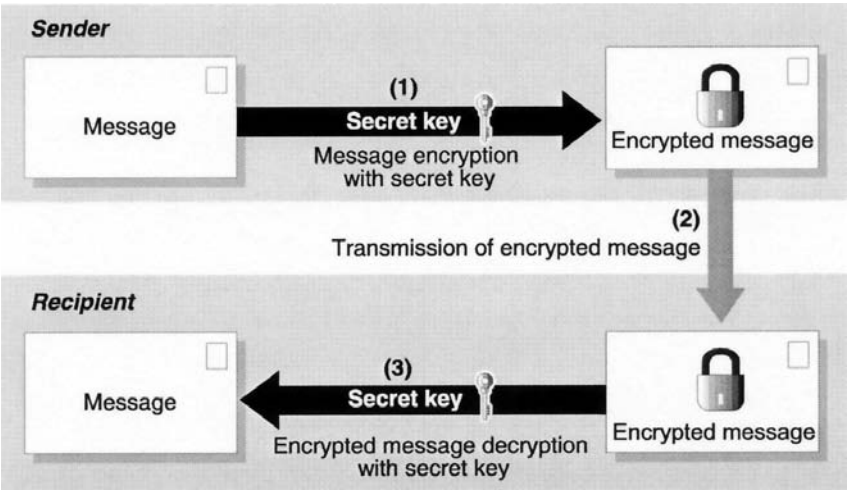

Figure 4.2 Symmetric-key cryptography

Various symmetric-key cryptography algorithms have been developed, in particular DES (data encryption standard), IDEA (international data encryption algorithm), series RC2 to RC6, and AES (advanced encryption standard).

DES (Data Encryption Standard)

The DES algorithm was jointly developed in the seventies by IBM and the NSA (National Security Agency). The DES is an encryption algorithm known as "by blocks." The length of the key used is fixed (40 or 56 bits). The purpose of the DES is to carry out a set of permutations and substitutions between the key and the text to be encrypted so as to encode the information.

The encryption mechanism follows several steps:

1. The text to be encrypted is divided into 64-bit blocks (8 bits are used for parity check).
2. The various blocks are subjected to an initial permutation.
3. Each block is divided into two 32-bit parts, a right part and a left part.
4. Sixteen rounds are performed on half blocks. A round is a set of permutations and substitutions. On each round, the data and the key are combined.
5. At the end of the sixteen rounds, the two right and left half blocks are merged and a reverse initial permutation is carried out on the blocks.

Once all the blocks have been encrypted, they are reassembled in order to create the encrypted text that will be sent over the network. Decryption is carried out in the encryption reverse order by still using the same key.

Until recently, the DES was the reference for symmetric-key cryptography. It was used and is still used by many systems. It is used by the information exchange protocol secured by SSL (secure sockets layer) Internet v1.0, for example, with a 40-bit key.

However, the DES hasn't been used since 1998 as its reliability was considered to be poor. Its encryption algorithm has been altered and improved.

3-DES

3-DES, or triple-DES, uses three DES one after the other. Therefore, the data is encrypted then deciphered then encrypted with two or three different keys. The size of the 3-DES key may be 118 bits in size. Because of this, it cannot be used in France. 3-DES is considered as being reasonably secure.

IDEA (International Data Encryption Algorithm)

The IDEA (international data encryption algorithm) is an algorithm with a 128-bit key length. The text to be encrypted is divided into four sub-blocks. Eight rounds are performed on each of these sub-blocks. Each round is a combination of exclusive "or," addition modulo 2^{16} and multiplication modulo 2^{16}. On each round, the data and the key are combined. This technique makes the IDEA particularly secure.

The IDEA is implemented in PGP (Pretty Good Privacy), which is the world's most widely used software.

RC2

The RC2 algorithm was developed by Ron Rivest, who gave it the name Ron's Code 2. It is based on an algorithm in 64-bit blocks. It is twice or even three times faster than DES with a maximum key length of 2,048 bits.

The algorithm is the property of RSA Security and is used in SSL v2.0.

RC4

RC4 (Ron's Code 4) no longer uses blocks but encrypts by stream. Its specific characteristic resides in the fact that it uses pseudorandom permutations for data encryption and deciphering.

Two mechanisms are defined by RC4:

- *KSA (Key Scheduling Algorithm)*. This algorithm generates a status table using the encryption key by means of simple permutations.
- *PRGA (Pseudorandom Generator Algorithm)*. The status table generated by KSA is placed in a pseudorandom number generator (PRNG) which creates the key stream by means of complex permutations.

Unlike the other algorithms, the data is not divided into blocks for their encryption or decryption. In RC4, the encryption corresponds to the addition of data to the key stream using an exclusive "or," whereas the decryption corresponds to the addition of encrypted data to the same key stream still using an exclusive "or."

RC4 is faster than RC2. Like RC2, it is the property of RSA Security. RC4 is used in SSL v2.0 and SSL v3.0 to secure connections and in the WEP protocol of IEEE standard series 802.11.

RC5 and RC6

RC5, another proprietary algorithm of RSA Security, is an encryption algorithm in blocks with a variable block size between 32 and 128 bits, a variable round number between 0 and 255, and a dynamic key length between 0 and 2,040 bits.

RC6 is an improved version of RC5 so therefore uses its characteristics. The only difference relates to the addition of new mathematical operations at the rounds.

Blowfish

Like DES, blowfish is an encryption algorithm in 64-bit blocks. Its key, based on DES, has a variable size between 40 and 448 bits. This algorithm is particularly fast and reliable.

Twofish

Like blowfish, twofish is an encryption algorithm in 128-bit blocks on 16 rounds with a variable key length. It is also both reliable and fast.

AES (Advanced Encryption Standard)

The AES is the result of a call for tender launched in 2000 by the NIST (National Institute of Standards and Technology) to replace the DES, which was seen as unreliable. Several algorithms were proposed, such as RC6 and Twofish, but Rijndael was chosen because it is simple and fast. Its name is now AES.

AES is an algorithm in 128-bit blocks, or 16 bytes, for K encryption key of 128, 192, or 256 bits. Depending on the key size, the number of rounds is 10, 12, and 14, respectively.

For each round, AES defines four simple operations:

- SubBytes, nonlinear substitution (S) mechanism that is different for each encrypted data block.
- ShiftRows, permutation (P) mechanism that shifts the block elements.
- MixColumns, transformation (M) mechanism that carries out a multiplication between block elements not in a conventional way but in a GF(2^8) Galois body.
- AddRoundkey, key derivation algorithm. It defines in each round a new encryption key, Ki, where i corresponds to the ith round from encryption key K.

The data is divided into 128-bit blocks before encryption. The first encryption stage consists of adding the data block with the encryption key by means of an exclusive “or.” Then, each block is subjected to ten rounds in a row, each made up of a substitution (S), a permutation (P) and a transformation (M). At the end of each round, a new encryption key is derived from the initial key, and the result of operation M is added to this key, Ki, by means of an exclusive ”or," all of which is sent to

the next round. At the end of the last round, which does not require transformation mechanism M, the data block is considered encrypted.

Once all the blocks for a given message are encrypted, they are reassembled in order to create the encrypted message that can then be transmitted over the network. The AES encryption procedure is illustrated in Figure 4.3.

Decryption is the opposite process of encryption as illustrated in Figure 4.4.

AES, which was used by the U.S. administration to replace DES, was also chosen as the new encryption algorithm for the IEEE 802.11i standard to replace RC4.

Public-Key Cryptography

The public-key cryptography technique solves the main problem with symmetric keys, which resides in the key transmission.

Two types of keys are used with public-key cryptography:

- A private key for data decryption. This key must remain confidential.
- A public key, which is placed at the disposal of all the users. This key is used for data encryption.

There is a mathematical link between these two keys, so finding the value of one of the two keys from the other one is very difficult.

The public key is sent over the network in plain text so it can be encrypted. The recipient uses his private key for data decryption as soon as the encrypted data has been received. This process is illustrated in Figure 4.5.

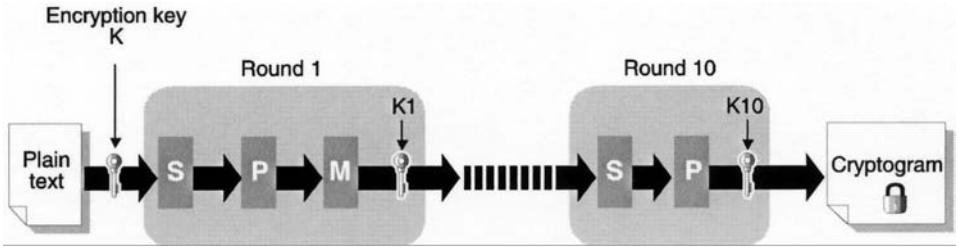

Figure 4.3 AES encryption

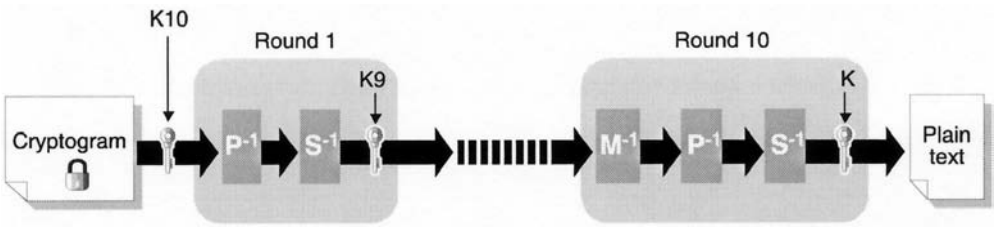

Figure 4.4 AES decryption

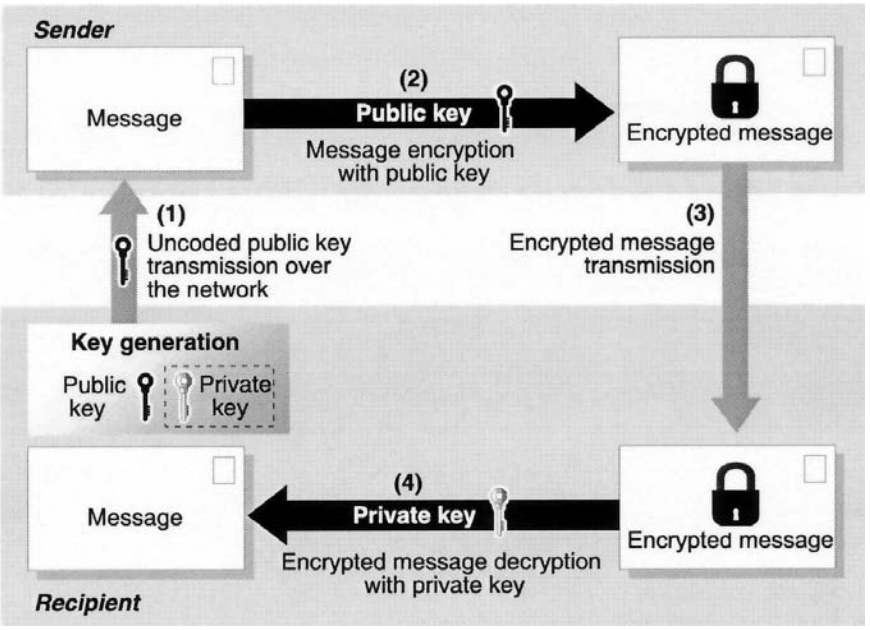

Figure 4.5 Public-key cryptography

As with symmetric-key cryptography, various algorithms are used, in particular RSA (Rivest, Shamir, Adelman) and Diffie-Hellman.

Though this technique makes it possible to compensate for the shortcomings of symmetric cryptography, i.e., key transmission, it is much slower than symmetric cryptography.

RSA (Rivest, Shamir, Adelman)

This public-key algorithm is named after its three inventors, Ron Rivest, Adi Shamir, and Leonard Adelman. RSA, which was created in 1977, was the first public-key algorithm. Its strength resides in the supposed difficulty to factorize large numbers.

RSA uses keys with a variable length (512, 1,024, and 2,048 bits). 512-bit keys are not considered to be very reliable. RSA is still used nowadays by SSL, IPsec, and many other applications. RSA is deemed reliable with reasonable key lengths until future mathematical advances are made.

Diffie-Hellman

This other public-key algorithm, which was invented by Whitfield Diffie and Martin Hellman, was the first encryption algorithm put on the market. As it is vulnerable to some types of attacks, it is preferably used with the help of a certification authority.

One of its characteristics is to enable two people to share a secret without requiring a safe transmission. It is still used today.

Mixed-Key Cryptography

Mixed-key cryptography, illustrated in Figure 4.6, uses the two aforementioned techniques, i.e. symmetric-key cryptography and public-key cryptography. It combines in this way the advantages of the two techniques while avoiding their disadvantages. Their disadvantages are well known, as symmetric-key cryptography does not enable secured key transmissions and the public-key cryptography uses algorithms that are too slow for data encryption.

When sending data, the sender encrypts the message with a secret key using a symmetric-key algorithm. At the same time, this secret key is encrypted by the sender with the public key generated by the recipient. The secret key can be transmitted reliably and securely in this way.

Encrypting a secret key on 128 bits using a public key algorithm is very fast considering the size of this key. It is then transmitted to the recipient. The recipient decrypts the secret key of the sender with his or her private key. The recipient now has the uncoded secret key and can use it to decrypt the message.

Another advantage of this technique is that it is no longer necessary to encrypt a message several times when it is intended for several recipients. As the encrypted message is transmitted with its secret key, all you have to do is encrypt this key with the various public keys of the recipients.

Electronic Signatures

The electronic signature is used to identify and authenticate the data sender. It is also used to check that the data transmitted over the network has not been changed.

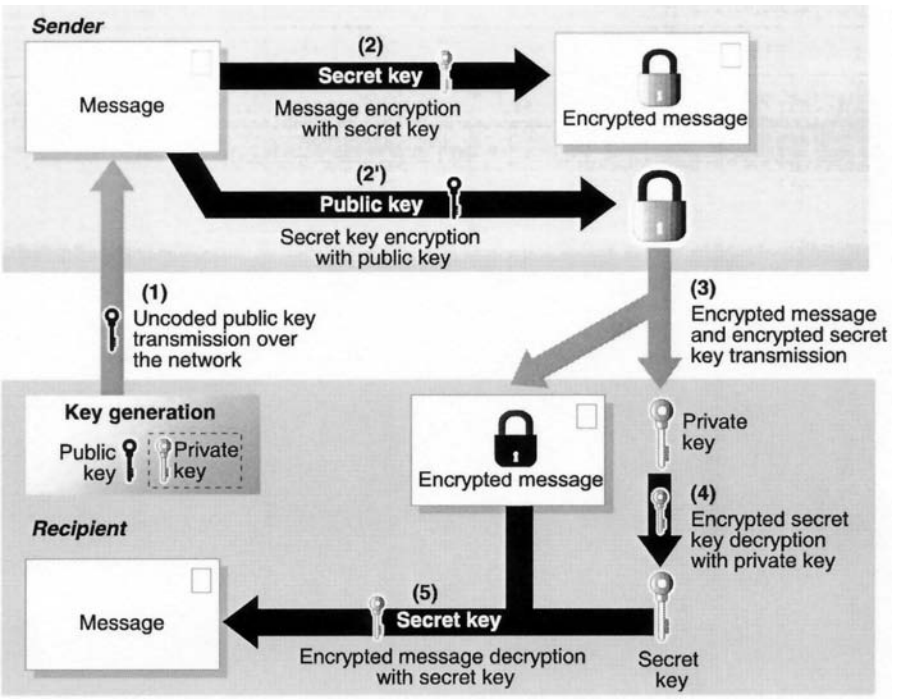

Figure 4.6 Mixed-key cryptography

A message to be sent can be signed using various techniques. One of them uses public-key algorithms but hash functions are mostly used.

Use of Public Keys

In addition to confidentiality, public-key cryptography has the advantage of allowing message sender authentications. The electronic signature is the second use for public keys.

For authentication purposes, the sender uses his or her private key to sign a message. The receiver uses the public key of the sender to make sure that the message has been signed. In this way, the receiver can check that the data has not been modified and that it has been sent by the sender.

Figure 4.7 illustrates how public-key authentication operates.

Although messages can actually be signed using this technique, confidentiality is not guaranteed, as the encrypted message and the public key may be intercepted and the data contents could be accessed.

The Hash Function

The hash function provides an alternative to the use of signatures using public and private keys.

The purpose of the hash function is to create a kind of digital digest of the message that must be sent. The size of this digest is very small compared with that of the message. Another characteristic of this technique is that it is very difficult, or even impossible, to find the original message again from its digest. This ensures the authenticity and integrity of the message sent.

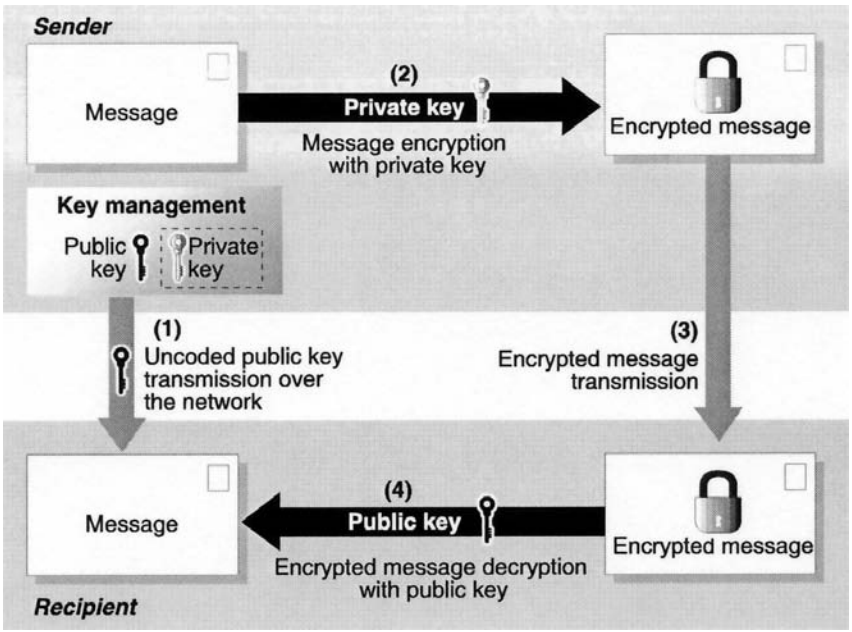

Figure 4.7 Public-key authentication

Figure 4.8 illustrates a sender who wishes to send a message while making sure of its authenticity. For this purpose, a message digest is created by the sender by means of hash function H. The message and its digest are sent to the recipient applying the same hash function H to the received message in order to compare the new digest with the received digest. If the digests are the same, this means that the message has not been modified.

MD5

On the Internet, we increasingly come across files to be downloaded with their digests, generally MD5, intended to check the integrity of the received data.

The hash function is often combined with public-key cryptography. The process is the following:

1. The sender hashes the message.
2. The digest is encrypted with the sender's private key.
3. The message, the public key of the sender, and the encrypted digest are sent over the network.
4. The recipient receives the message, which he hashes in turn to extract a new digest from it.
5. This digest is compared with the digest he has received in the encrypted condition. The digest is decrypted by the recipient using the public key provided by the sender.
6. If the two digests match, the message is authenticated.

This process is illustrated in Figure 4.9.

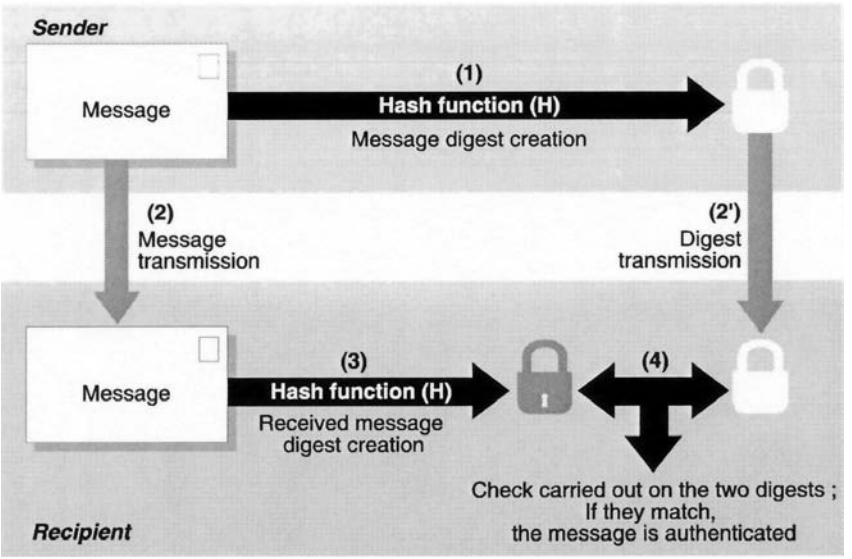

Figure 4.8 Message hash

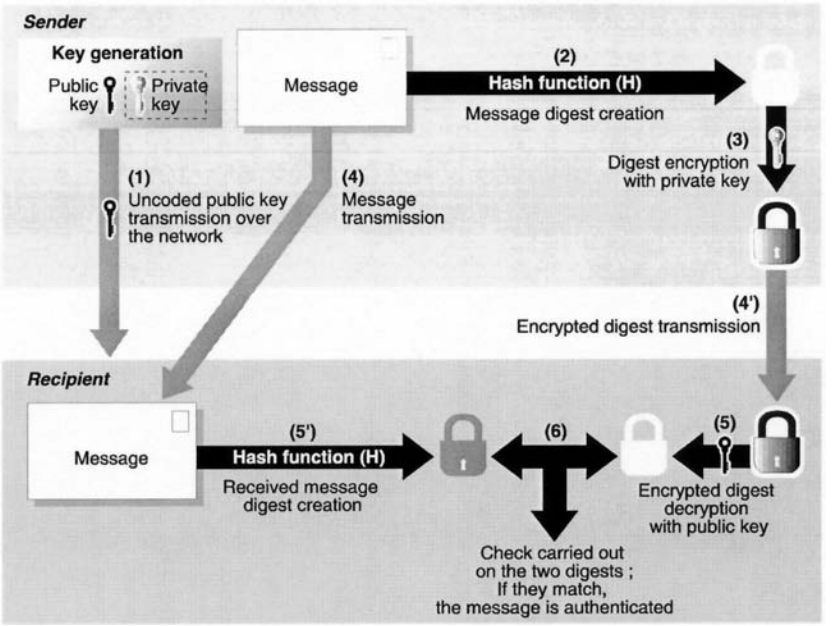

Figure 4.9 Hash and public key

Various hash techniques are used, in particular the following ones:

- *MD2, MD4, and MD5*. Message digests 2, 4, and 5 were developed by Ron Rivest for RSA Security. These are hash functions that all produce digests with a size of 128 bits. MD2 is the most reliable but is optimized only for 8-bit machines, whereas the other two are optimized for 32-bit machines. MD4 was abandoned since it is too sensitive to certain attacks. MD5 is an evolution of MD4. It is considered as reliable, even if it is vulnerable to certain attacks, and is used in many applications. MD5 has been standardized by IETF under RFC 1321.
- *SHA and SHA1*. SHA (Secure Hash Algorithm) and its evolution were developed by NSA. These two algorithms produce 160-bit digests for a message which may reach a size of two million terabytes. The size of its digest makes it very difficult to crack, but it is slower than MD5 Network attacks.

The networks have been subjected to various types of attacks at all times. These may be passive attacks, like in the case of listening to a network for the purpose of recovering information by "cracking" the various passwords and encryption keys. In other cases, these are active attacks. The attacker attempts to take control of machines or to damage some machine devices.

The most common attacks are the following:

- *Denial of service (DoS) attack*. This attack, which is among the most feared, consists of flooding a network with messages so that the network devices can no longer process them, sometimes up to the point of collapse.

- *Brute force attack*. This attack consists of working through all the possible combinations in order to recover a password or an encryption key used in a network.
- *Dictionary attack*. This attack is used to recover a password or a key by using a database containing many words.
- *Spoofing attack*. This attack is based on identity usurpation in order to access the network. It is generally associated with brute force or dictionary attacks that are used to access certain information, like the login and password of a user.
- *Attack on exploiting holes in security*. Many protocols and operating systems are vulnerable due to their design. These flaws can be used either to make it possible for the attacker to get into the machine or in the network, or to gain control of the machine or recover data.
- *Virus, worm, and Trojan horse attacks*. These attacks are very well known and make it possible either to damage files or even machine components, or to gain control of a machine (viruses and worms) and to exploit its resources (Trojan horse).

Security for PLC Networks

HomePlug implements a PLC private network system based on encryption keys known by authorized PLC devices in this network for increased PLC network security.

This mechanism is based on the secure, reliable, and simple registration for the network manager or user of the various PLC devices of the same logical network. These functionalities make the deployment of PLC networks easier.

The main characteristics of the registration of a PLC device in a PLC network are the following:

- *Security*. A device can be registered in a PLC network only if it has the suitable encryption keys and only if it is authorized and registered by the network managing devices. It must be possible to easily attach new devices and also to quickly remove devices from a PLC network.
- *Reliability*. The same PLC network must provide stability in the configuration of encryption keys and support the electrical connections/disconnections of the network PLC devices in a stable manner. It must also be possible to recover an original configuration if the keys are lost or if a device is deconfigured.
- *Simplicity*. Managing the configuration of the encryption keys of the various PLC logical networks must be simple for a network manager. For this purpose, a single key used for data exchange encryption over the electrical network is defined by HomePlug 1.0 and Turbo. HomePlug AV, which is more sophisticated, defines several network keys that are managed by the network coordinating device that centralizes the keys.

Therefore, a PLC logical network is based on an encryption key called a NEK (network encryption key) in the HomePlug specification that encrypts the data exchanged between the various PLC devices (see Figure 4.10).

A PLC network can be configured with a NEK in several ways:

- *Via the Ethernet interface.* A configuration frame of the NEK is sent in broadcast mode to the PLC devices of the same network using a configuration tool. All the PLC devices connected by means of their Ethernet interface recover this configuration.
- *Via the electrical interface.* A configuration frame of the NEK is sent by means of the electrical network to the connected PLC devices. This is only possible if a second key, called DEK (default encryption key) is known. This key, which is specific to each PLC device, is recorded in the device memory by the manufacturer by following HomePlug specifications. The DEK is used by two PLC devices—the configuring station device and the device which must receive the new NEK—for the encrypted NEK exchange over the electrical network.
- *Via a Web interface.* If the PLC devices are advanced, like those of the Asoka USA brand, the key configurations can be managed by a single Web interface.

Access to the Physical Medium

In Wi-Fi, the transmission medium is shared. Therefore, anyone in the network coverage area can intercept its traffic or even reconfigure the network at will. In addition, if a malevolent person is rather well equipped, this person does not need to be in the network coverage area. The person just has to use an antenna with or without amplifier assistance to have access to it.

In the case of PLC, the transmission medium is also shared, but the access to the physical medium is much more difficult and especially potentially dangerous.

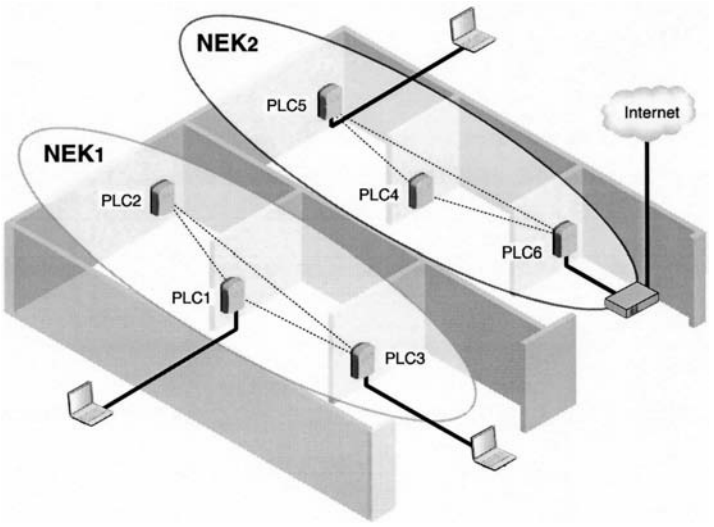

Figure 4.10 PLC logical networks with various NEK

However, several more or less realistic techniques are used to have access to the data exchanged over a PLC network; in particular, these techniques consist of:

- Using a PLC device with the suitable NEK key for the targeted network.
- Recovering the physical data via the electromagnetic radiations emitted by the PLC network in the environment close to the electrical wiring. However, this requires a complex and costly acquisition chain.
- Constructing a specific PLC device capable of recovering the encrypted physical frames in order to attempt to decrypt them.

Figure 4.11 illustrates the internal design of a PLC device with its two interfaces: on the one hand, the Ethernet interface connected to an Ethernet network where uncoded frames circulate; and on the other hand, the PLC interface connected to the electrical network where encrypted frames circulate.

A PLC device consists of an electrical interface that sends and receives the frames over the electrical network, and of an Ethernet interface (RJ-45 connector), which sends and receives frames over the Ethernet network. Between these two interfaces, the data only flows if the device has the right NEK from the PLC network.

If a PLC device does not have the network NEK, the Ethernet frames are not available on the Ethernet interface. Therefore, the encrypted PLC frames cannot be accessed easily.

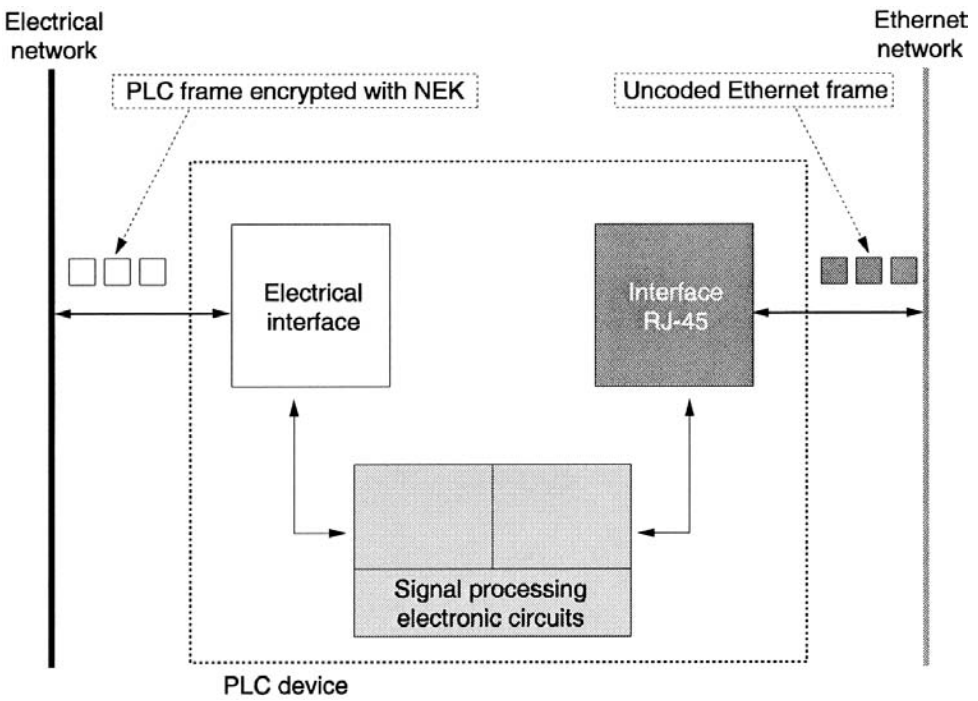

Figure 4.11 Internal design of a PLC device used to encrypt exchanged frames

Access to Physical Frames

The data exchanged over a PLC network is carried in PLC frames known as "physical frames."

The PLC frames circulate over the electrical network between all the outlets in encrypted form. As explained above, it is difficult to have access to the physical medium. Because of this, the frames are relatively protected from attacks intended to accumulate enough frames to try them out with a brute forcing tool intended to try out all the combinations or using various decryption algorithms.

In addition, the PLC frames are carried in several frequency bands; each of these bands may use various information transport techniques, i.e., binary data modulation techniques over the transmission channel.

As we have seen in Chapters 2 and 3, the various network PLC devices permanently adapt their digital transmission technique according to the quality of the PLC links, i.e., the capacity of the transmission channel in terms of bit rate. For this purpose, the tone map indexes the links between the PLC device storing it and all the other network PLC devices.

To have access to the physical frames, it is therefore necessary to continually know this tone map in order to identify the technique used to transport information between the network PLC devices.

Authentication

The authentication of a PLC device consists in knowing the NEK that identifies the network to which it belongs. If a PLC device does not have the right NEK, it cannot exchange data with the devices of the PLC network to which it wishes to connect.

Figure 4.12 illustrates the main steps relating to the access of a PLC device to a network identified by the NEK (network encryption key) of HomePlug 1.0 and Turbo. This NEK, called here NEK2, is the identifier of the PLC network since only the PLC devices that have a configuration with this key belong to this network.

Certain more advanced PLC devices, like those of the Asoka brand, are used to create an authentication of the devices concerning the MAC address in addition to the NEK key. This authentication is managed from the network administration interface by means of a list of MAC addresses which may belong to the PLC network.

Network Keys

In a computer network, the network keys are used to protect the exchanged data by encrypting it before sending this data over the network. In a PLC network, the data flows over the electrical network, which is a shared network. Therefore, it is important to encrypt the data to avoid data recovery. For this purpose, the PLC networks use keys that make it possible to identify a network and all the PLC devices belonging to it.

In HomePlug 1.0, there are two encryption keys, NEK and DEK, stored in a register specific to each device and accessible via the EKS (encryption key select) parameter.

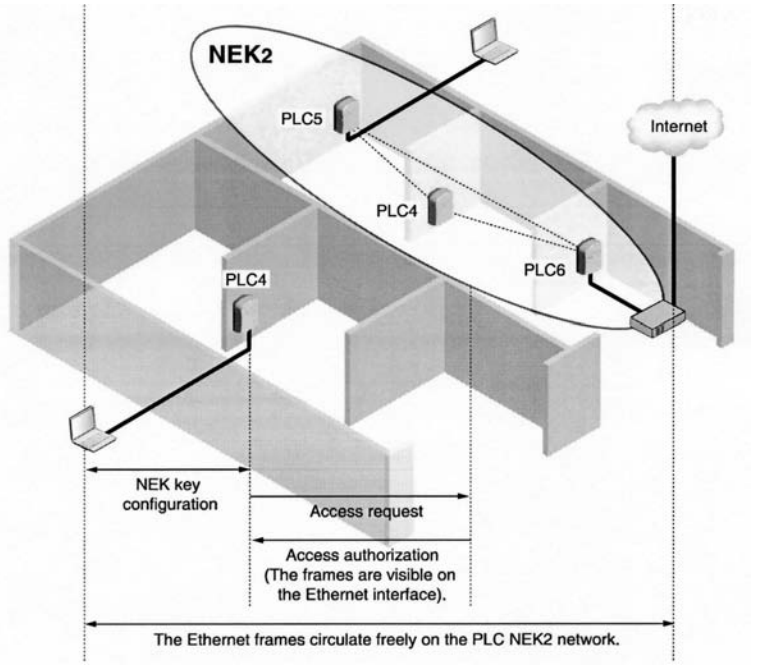

Figure 4.12 Access of a device to a PLC network identified by its NEK key

The NEK identifies the PLC network in the same manner as the WEP (wired equivalent privacy) is used to protect the data of a Wi-Fi network. It also carries out the following tasks:

- creation of several PLC networks on the same electrical network;
- encryption of the data flowing between the PLC devices; and
- authentication of the devices belonging to the PLC network.

Default NEK of HomePlug PLC Networks

In HomePlug, the default NEK is equal, in ASCII, to 0x46D613E0F84A764C, which is equivalent to the word HomePlug. Any HomePlug PLC device available in stores is configured with this encryption key.

If a non-trained user tries to make its equipment work in this way without network configuration notions, the price to pay is the total absence of security, insofar as all the devices complying with this standard are capable of recovering the data exchanged over the electrical network irrigating a building or a single family house.

The DEK identifies a particular PLC device. It is used for the remote configuration of PLC devices via the electrical network of the house or business wiring.

This key is used to create an encrypted communication between the PLC device holding the NEK and the PLC device trying to belong to the PLC network.

As we'll see in Chapter 9, dedicated to practical PLC network configurations, this key can prove very useful for remote device configuration from a network administration central point.

Calculating the NEK

The PKCS#5 standard specifies two methods for the implementation of a cryptography derived from passwords. The PBFDK1 method was chosen in HomePlug. As input parameters, it demands a password (entered by the administrator); a "salt value" (constant parameter specified by HomePlug which is a kind of public key); an iteration count, i.e. the number of times that the operation specified in the PBFDK1 formula will be reiterated in a loop for greater encryption efficiency; and the length of the output derived key.

The PBFDK1 method uses the MD5 hash function used for the synthetic and unique definition of the encrypted message digest, in this case the encryption and the digital digest of the PLC network password.

It is described by the following function:

$$DK = PBFDK1\ (P, S, c, dkLen)$$

where:

- DK = derived key (with dkLen set to 8, DK is NEK);
- P = password (entered by the network administrator);
- S = salt value (equal in ASCII to 0x0885 6DAF 7CF5 8185);
- c = iteration count (1,000 times);
- dkLen = length in bytes of derived key (8 bytes).

According to the FIPS PUB 112 standard, the usage rules concerning passwords consist of defining a length between 4 and 8 bytes, even if longer passwords (up to 24 bytes) are possible.

PBFDK1 specifies that the hash function (MD5) must be applied 1,000 times in an iterative manner by using the results of the preceding iteration. The first value is the concatenation of the password and salt value.

The iterative process occurs in the following way:

T_1 = MD5 (P|S)
T_2 = MD5 (T_1)
…
$T_{1,000}$ = MD5 (T_{999})
DK = $T_{1,000}$ <0…7>
where (P|S) is a concatenation of P and S.

MD5 Algorithm (RFC 1321)

The MD5 algorithm produces a 128-bit message digest (MD) from an input message. In theory, the same MD cannot be obtained for two distinct messages.

The MD5 algorithm can be summarized in the following way:

$m_{ext} = m + m_{pad} + m_l$

where

m_{ext} is the extended message produced by the MD5 algorithm.

m is the input message of arbitrary length converted to a bit stream.

m_{pad} consists of pad bits (1 followed by 0's) concatenated to m such that the length of m_{ext} is congruent to 448, modulo 512.

m_l is the length, in bits, of the original message, m, expressed as 64-bit binary blocks.

The extended message, m_{ext}, is subjected to four rounds of bit transformations where each transformation includes 16 operations. On each operation, a fixed value is added to the result. This fixed value added to each result of the 64 operations (different value for each operation) is calculated using a SINE function and stored in a 64-row table (one row for each operation).

A fixed value calculated in the following way is therefore stored on each row:

Addition = int(2^{32} × abs(sin(i)))

where i is expressed in radians.

These 64 fixed numbers (addition) will never exceed 32 bits.

Security in HomePlug AV

The main security functionalities implemented in HomePlug AV are the following:

- Encryption based on 128-bit AES in CPC (cipher block chaining) mode;
- Data protection using a NEK (rotation of NEK values every hour) encrypting the physical data;
- Authentication to join a PLC network using a NMK (network membership key) used to distribute NEK over the network;
- New PLC device authorization by configuration:
  - using a frame carrying the NMK over the Ethernet interface;
  - using a DAK (direct access key) key corresponding to the DEK key of HomePlug 1.0;
  - using the easy connect button;
  - using a MDAK (Meta DAK);
  - using a pair of PPK (public-private key encryption);
- Support of HLE (higher layer entities) protocols, such as IEEE 802.1x.

Table 4.1 summarizes the security management characteristics of the various PLC technologies with their key management, encryption level, advantages, and disadvantages of each method.

Attacks

As we have seen at the beginning of the chapter, the purpose of an attack is not restricted to the connection to a network in order to recover data via flaws in it. An attack can also be intended to disturb network operation, both at the network and physical levels.

Table 4.1 Encryption-Key Management According to PLC Technology

TECHNOLOGY	*KEY MANAGEMENT*	*ENCRYPTION*	*ADVANTAGES*	*DISADVANTAGES AND FLAWS*
HomePlug 1.0	NEK	DES-56 bits	Simplicity	– DES shortcomings – A single key for each device
HomePlug Turbo	DEK	Same	Same	Same
HomePlug AV	– NEK – NMK – DAK	AES-128 bits (key rotation)	High encryption level	Possible shortcomings with easy connect button
Ascom	Key exchange	RC4 + Diffie-Hellman (128 bits)	Configuration made easier by interface	RC4 shortcomings
DS2	Master-slave key exchange	3DES	Central configuration by administration console on master device	Interception of key exchanges during authentications
Oxance	– NEK – DEK	– DES-56 bits – AES-128 bits	Management by Web centralized interface	Possible Web interface shortcomings

Decryption Attacks

The purpose of this attack is to try to discover the NEK of a PLC network in order to connect to it and to recover the exchanged data.

The two following techniques are used to discover the NEK in HomePlug 1.0:

- Have access to the physical frames and store enough frames so that they can be decrypted using suitable algorithms. However, this technique is very complex and requires expensive specific hardware solutions.
- Try out all possible combinations of NEK to have access to the network.

The time that is necessary to try out all the possible combinations of NEKs can be estimated in the following way: the NEK is encoded with the DES-56-bit algorithm derived from a password entered by the user of the PLC network, which may vary from 4 to 24 characters.

Therefore, the maximum number of possible attempts is:

$$N = 2^{58} \approx 2.88 \times 10^{17}$$

For a 64-byte Ethernet frame with a 100-Mbit/s network interface card, the transmission time is:

$$T_{frame} = \frac{64 \times 8 \text{ bits}}{100 \times 1{,}024 \times 1{,}024} \approx 4.88 \times 10^{-6} \text{ sec}$$

The total time which is necessary to try out all combinations then is:

$$T_{total} = N \times T_{frame} = 2.88 \times 10^{17} \times 4.88 \times 10^{-6} \approx 1.4 \times 10^{12} \text{ sec} \approx 44{,}591 \text{ years}$$

We notice that this technique requires too much time to be used efficiently.

Denial of Service Attacks

The purpose of an attack is not necessarily to crack an encryption algorithm to recover the key and listen to the network or get into it. The single purpose of some attacks is to sabotage the network by preventing it from operating. This type of attack, called denial of service, or DoS, is widespread for all network types.

In PLC networks, the simplest denial of service corresponds to scrambling. Since these networks operate in the 1- to 30-MHz frequency band, the use of a radio unit using the same band with a power greater than PLC power can cause interference and, consequently, a global performance drop; it can even completely prevent the network from operating. This attack is the simplest to implement. Unfortunately, it is also unmanageable.

IEEE 802.1x and Improvements to PLC Network Security

IEEE 802.1x is an authentication architecture proposed by the IEEE committee 802. This is not in any case whatsoever a completely separate protocol but these are guidelines used to define the various functionalities that are necessary to implement a client authentication service on any type of local area network (Ethernet, PLC).

The 802.1x architecture, called port-based network access control, is based on two key elements, the EAP and RADIUS protocols.

The port is an important element of this authentication architecture. The port defines any type of attachment to a local area network infrastructure. In PLC, like in Ethernet, the connection of two machines is considered as a port.

The 802.1x architecture is illustrated in Figure 4.13. It consists of the three following distinct elements:

- a client corresponding to the user who would like to connect to the network via his or her station;
- a controller, generally a switch or a router, relaying and controlling the information between any requester and the authentication server;
- an authentication server authenticating the user.

For each port, the network traffic can be controlled or not. Between the client and the controller, the port is controlled so that only EAP authentication messages of the request-response type are transmitted. Any other type of traffic is rejected. On the contrary, between the controller and the authentication server, any type of traffic is accepted since the medium is supposedly secure.

In 802.1x, the authentication is based on the EAP (extensible authentication protocol) and the use of a RADIUS (remote authentication dial-in user service) server.

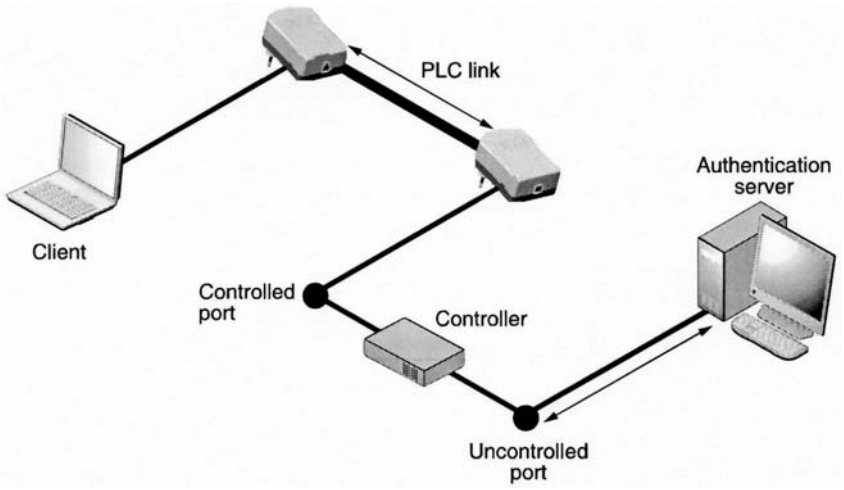

Figure 4.13 IEEE 802.1x authentication architecture

RADIUS and Diameter

802.1x does not define a particular authentication protocol on the server side. Two client-server authentication protocols, RADIUS and Diameter, can be used. The simplest one, RADIUS, has become the default server of any 802.1x architecture. The main constraint of diameter is that it is based on the SCTP (Stream Control Transmission Protocol) transport layer which is not implemented as much as TCP.

EAP (Extensible Authentication Protocol)

EAP was defined originally for the PPP (point-to-point protocol) as an extension to the existing PAP (password authentication protocol) and CHAP (challenge handshake authentication protocol). Compared with these two protocols, EAP provides many authentication methods in a relatively simple way. This simplicity is due to the fact that EAP is only an envelope for the transport of these authentication methods.

Within the framework of a 802.1x PLC architecture, five EAP authentication methods are used:

- *EAP-MD5*. This solution is based on the hash function (MD5). For authentication, the user gives a login-password, the MD5 digest of which is transmitted for authentication purposes to the server. This solution is deemed not to be very reliable though only the digest is transmitted over the network and not the login-password. It is no longer supported by Windows XP SP1.
- *EAP-TLS*. TLS (transport layer security) is a mechanism used to implement a secured connection. The mutual authentication between the client and the server, the data encryption, and the dynamic management of keys constitute its functionalities. TLS is the basis of SSL 3.0, which is found in HTTPS, a protocol used by many Web sites (banks, online reservation sites, and so forth).

Apart from encryption, EAP-TLS has the same characteristics as TLS but these are encapsulated into EAP packets.

- *EAP-TTLS*. EAP-TTLS (tunneled TLS) is a Funk Software solution based on the use of two tunnels; the first one is used for authentication purposes by EAP-TLS and the second one to secure transmissions with an authentication method left to the choice of the manufacturers (EAP-MD5, PAP, CHAP, and so forth).
- *PEAP*. Protected EAP is a solution proposed by Microsoft, RSA, and Cisco Systems. Like EAP-TTLS, PEAP is based on two tunnels but the two tunnels use EAP-TLS as the authentication method.
- *LEAP*. Lightweight EAP, which is proposed by Cisco, corresponds to a lightweight version of the preceding solutions but with the same functionalities, mutual authentication between the client and the server, and dynamic management of the keys.

Although these solutions are based on a mutual authentication between the client and the server, sometimes with an additional authentication method for secured data transport, these are not flawless. The MIN (man in the middle) attack makes it possible, for example, for an attacker placed between the client and the server, i.e., in the middle, to recover the messages and hijack the identity of a client to authenticate himself in his place.

To conclude, 802.1x is a solution used to improve the security of PLC networks by adding to the management of NEK securing the physical frames on the electrical network.

RADIUS (Remote Authentication Dial-in User Server)

RADIUS is a centralized user authentication and authorization protocol. Originally designed for remote access, it is currently used in many environments, such as VPN and Wi-Fi access points, and has become a IETF standard (RFC 2865).

Situated above level 4 in the OSI architecture, it uses the UDP transport protocol for obvious reasons fastness and is based on a client-server architecture.

As illustrated in Figure 4.14, the client sends server connection attributes. The authentication between the server and the client is done by means of a shared secret, which generally consists of a key and of the client attributes. For authentication purposes, the server sends a challenge to the client that can only be solved by the shared secret. It checks the attributes sent by the client and the response to the challenge and accepts the client if they are correct.

IEEE 802.1x in PLC

EAPoL (EAP over LAN) is the EAP version used within the framework of Ethernet and Wi-Fi local area networks like PLC. It appears as an Ethernet encapsulation viewed from the link between the client terminal and the RADIUS server.

The exchange of EAPoL messages for the authentication of a station to an access point is illustrated in Figure 4.15.

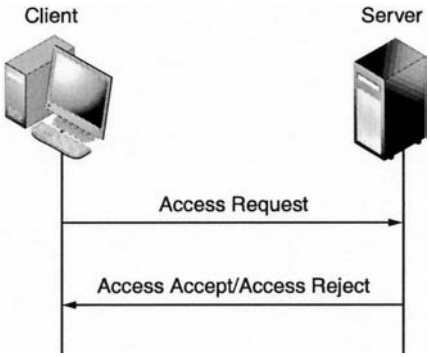

Figure 4.14 RADIUS negotiation

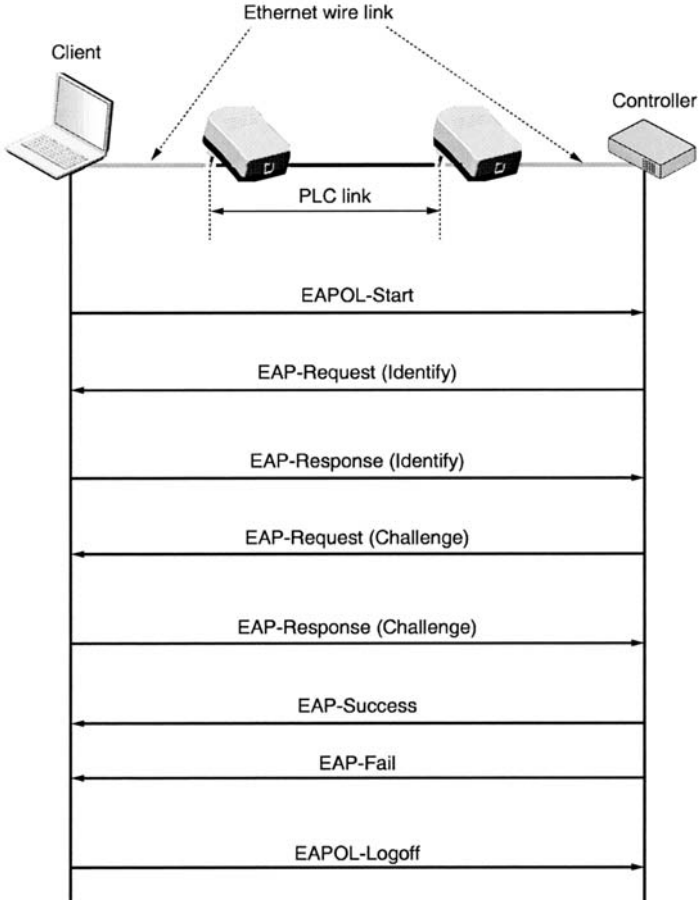

Figure 4.15 Exchange of EAPoL messages between an access point and a station

The authentication is always initiated by the station which sends an EAPoL-Start request. The access point transmits to it one or several requests to which it must respond. The authentication phase ends either with an EAP-Success message, which guarantees that the station is authenticated, or with an EAP-Failure

message; in this case, the station is not authenticated. The station can deauthenticate itself at any time by sending an EAPoL-Logoff request.

802.1x uses an authentication server to which the access point relays information, as shown in Figure 4.16. The authentication phase can only be initiated by the station. After having received the authentication request, the access point requests the station to identify itself with an EAP-Request (Identity). As soon as the station identifies itself at the access point with an EAP-Response (Identity), this request is transmitted to the authentication server (Access Request).

In general, the station and the authentication server share a secret (key, login password, certificate) that depends on the authentication method used. As soon as the authentication server receives a request from a client (a station) connected to the PLC network, it sends an Access Challenge message containing a challenge to the station. This challenge can only be solved by the secret shared between the station and the authentication server. If the challenge is not solved, the station cannot authenticate itself; if it is solved, the authentication server authenticates the station, which can from then on connect to the network via the controlled port located between it and the PLC device used to have access to the PLC local area network.

Any type of server supporting EAPoL can be used as the authentication server. However, the most widespread server still is RADIUS.

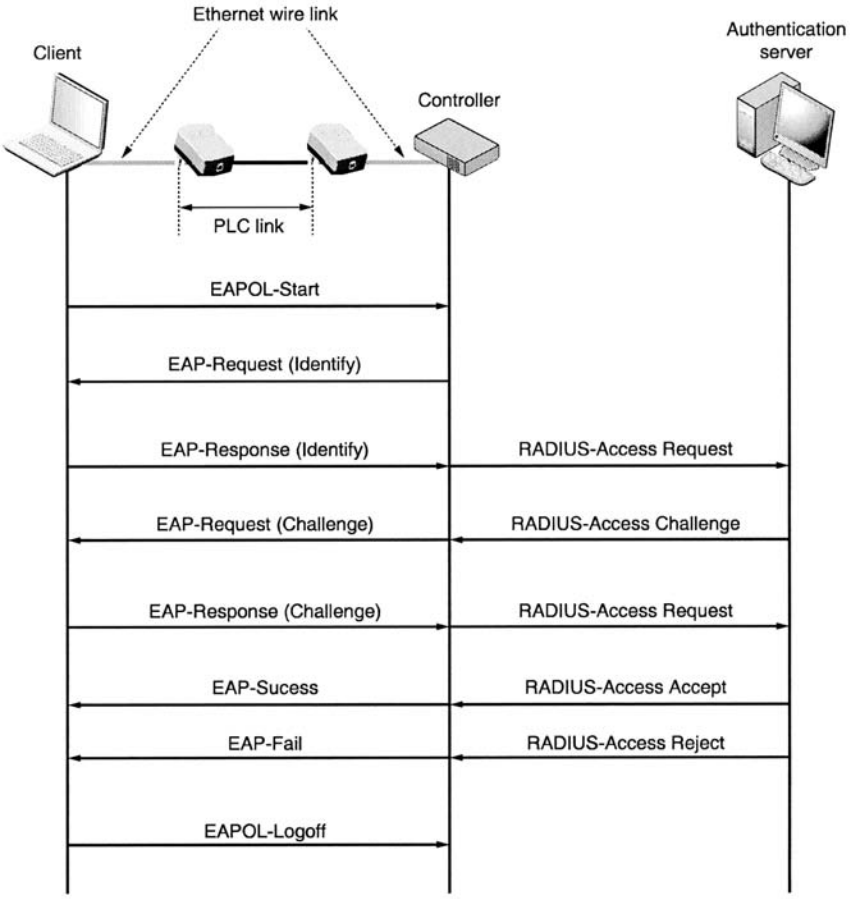

Figure 4.16 Authentication phase in IEEE 802.1x

Virtual Private Networks

The purpose of the virtual private networks, or VPN, is to provide an end-to-end secured tunnel between a client and a server. VPN are used, among other things, to identify and to authorize access as well as to encrypt any traffic flowing in the network.

To date, IPsec is the protocol that is the most used in VPN. IPsec, the reference standard, is based on various protocols and algorithms according to the desired security level:

- authentication by public-key electronic signature (RSA);
- integrity control by hash function (MD5);
- confidentiality by means of symmetric algorithms, such as DES, 3DES, AES, IDEA, blowfish, and so forth.

The use of a VPN is the most reliable way to secure a wireless network. This method is also the most used.

CHAPTER 5

Frames

To send information, the PLC stations must prepare data frames, i.e., data blocks with a header and an area indicating the end of the frame. The block containing the user data has a specific format that depends on the technique used in order to access the physical medium used. As the power line medium is shared, a technique used to circulate multiple frames coming from various machines must be determined. This frame structure sent over the physical layer is completed by a second frame structure encapsulated into the first one.

Figure 5.1 illustrates the transmission of data in the architecture with PLC access via the MAC (data link) and physical (PHY) layers. The first layer corresponds to the technique used to access the power line medium. The frame corresponding to this protocol is called the MAC or MPDU (MAC Protocol Data Unit) frame.

All the data coming from layers above the MAC layer is encapsulated into the MAC frame. This MAC frame is encapsulated into a second physical layer frame in order to convey the frame over the physical interface or electrical interface. This frame is called PPDU (physical protocol data unit).

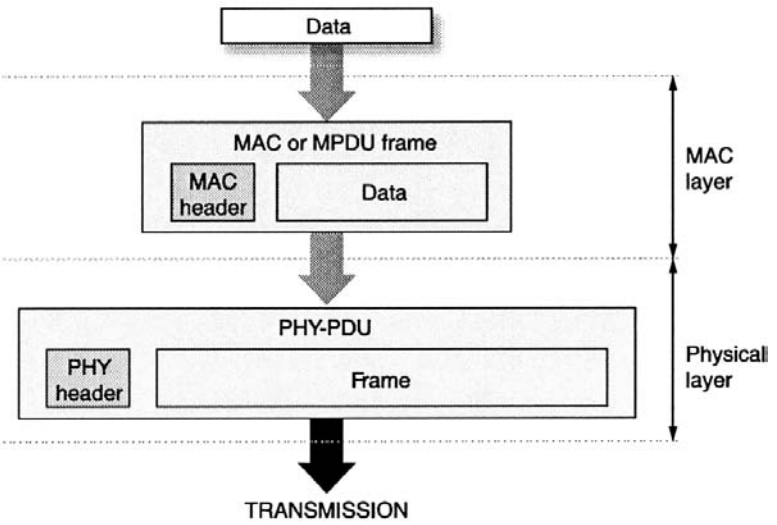

Figure 5.1 Data transmission in PLC access architecture

This chapter discusses the structure of the PLC frames used in HomePlug 1.0 and introduces the main characteristics of the frames in HomePlug AV.

Physical Layer Frames

If we observe the complete structure of the HomePlug 1.0 physical layer frame permanently exchanged between the PLC devices (see Figure 5.2), we notice that it consists of a number of elements surrounding the long data frame including the data of the higher level protocol layers from the OSI model's point of view.

In terms of time length, the HomePlug 1.0 frame can be quantified by minimum and maximum values, with a fixed part (header), a variable data part, and a part used for contention periods with regard to the CSMA/CA process as indicated in Table 5.1.

Therefore, the HomePlug 1.0 frame consists of "long" data frames, which comprise the data of the MAC frames, and "short" data frames, which comprise response information from the other PLC devices.

Remember that the average time of a HomePlug 1.0 frame is 1,600 μs.

From the point of view of the physical layer modulation techniques, the HomePlug 1.0 data frame consists of OFDM (orthogonal frequency division multiplexing) symbols. These symbols form blocks that, in turn, constitute the complete frame.

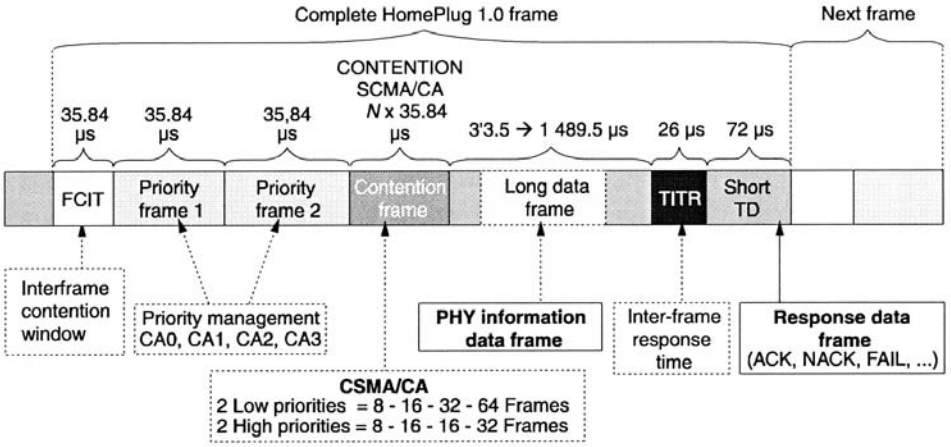

Figure 5.2 HomePlug 1.0 frame structure

Table 5.1 HomePlug 1.0 Frame Time Length

	FIXED (HEADER)		*VARIABLE (DATA)*		*CONTENTION (CSMA/CA)*		*TIME LENGTH*
MIN	205.52 μs	+	313.5 μs	+	$N \times 35.84$ μs	=	519.02 μs + ($N \times 35.84$ μs)
MAX	205.52 μs	+	1,489.5 μs	+	$N \times 35.84$ μs	=	1,692.02 μs + ($N \times 35.84$ μs)

Figure 5.3 illustrates the respective times of these various OFDM blocks.

The complete frame time is defined by adding the various OFDM symbol block times. The maximum possible transmission speed and the bit rate concerning the data link layer can be calculated in this way.

With a 2,705-byte frame, the maximum transmission speed is obtained in the following way:

$$\text{Bit rate}_{\text{PHY\_MAX}} = 2{,}705 \times 8 \text{ bits}/1{,}534.86\ \mu\text{s} = 14.1 \text{ Mbit/s}$$

With an Ethernet data frame with a maximum length of 1,500 bytes, the maximum bit rate is the following:

$$\text{Bit rate}_{\text{PHY\_MAX}} = 1{,}500 \times 8 \text{ bits}/1{,}534.86\ \mu\text{s} = 7.81 \text{ Mbit/s}$$

Table 5.2 summarizes the maximum theoretical transmission speeds in the HomePlug 1.0 standard. As we'll see in part II of the book, these values are lower in practice.

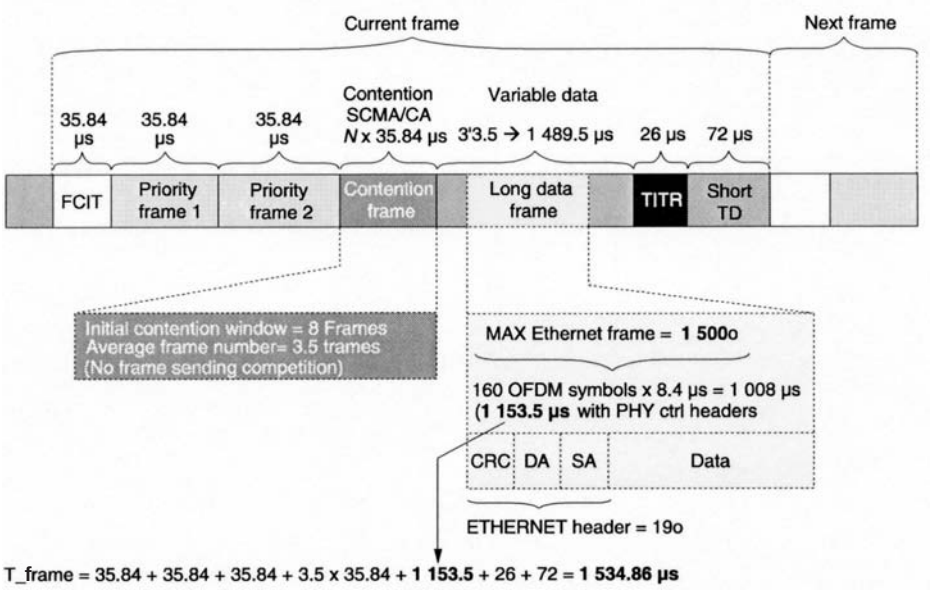

Figure 5.3 Complete HomePlug 1.0 frame OFDM symbol block times

Table 5.2 Maximum Transmission Speed According to Modulation Technique

MODE	*ERROR CORRECTION CODE (FORWARD ERROR CORRECTION)*	*MAXIMUM TRANSMISSION SPEED IN THEORY (Mbit/s)*
DQPSK ¾	¾ convolution code and Reed-Solomon code	14.1
DQPSK ½	½ convolution code and Reed-Solomon code	9.19
DBPSK	Convolution code and Reed-Solomon code	4.59
ROBO (DBPSK ½), repetition of each bit four times	½ convolution code and Reed-Solomon code	1.02

Improved transmission speeds are predicted with the evolution of PLC technologies, as indicated in Table 5.3.

Architecture of the Physical and Data Link Layers of HomePlug AV

The latest technical developments by the HomePlug consortium have led to improvements in HomePlug 1.0 performance in the new HomePlug AV version.

The architecture of the physical layer and of the data link layer has been modified while allowing interoperability with the HomePlug 1.0 devices in order to authorize the master-slave mode.

Figure 5.4 illustrates the architecture of these two layers.

Two simultaneous functions are managed by these layers: management of checks between the master and the slaves of the network, mainly to provide the various QoS functionalities, and data management to encapsulate MAC and to make data in the upper layers available.

Table 5.3 Forecast Maximum Transmission Speed of Various PLC Technologies

PLC TECHNOLOGY	*FORECAST TRANSMISSION SPEED*
HomePlug Turbo	85 Mbit/s
HomePlug AV	200 Mbit/s
Spidcom SPC200-e	220 Mbit/s
DS2	200 Mbit/s

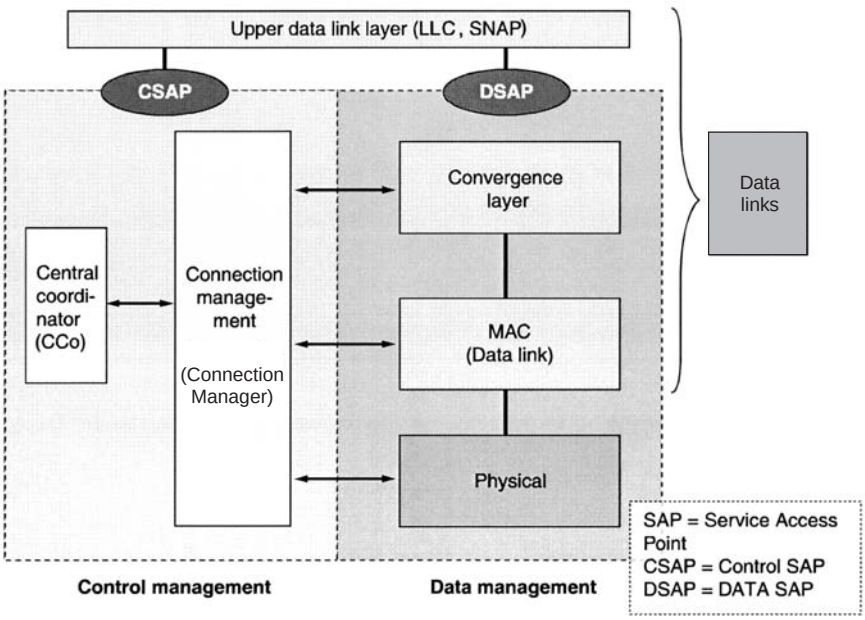

Figure 5.4 HomePlug AV architecture

The OFDM Interface Frame

The OFDM (orthogonal frequency division multiplexing) interface is the access technique used by PLC. This access technique is also used by Wi-Fi in the IEEE 802.11a and 802.11g standards and by the ADSL and terrestrial TV broadcasting technologies.

This technique is highly robust with regard to communication media interference. The OFDM technique principle is to separate the frequency band into narrow sub-bands, with each sub-band transporting part of the binary information. The frequency responses of each sub-band are orthogonal and slightly overlap to obtain good spectral efficiency.

OFDM Symbols

As explained above, the HomePlug 1.0, Turbo, and AV frames consist of OFDM symbols of binary data combined into blocks.

Figure 5.5 gives a temporal and frequencies representation of the OFDM frequency bands used by PLC technologies. The frequency band is divided into 84 sub-bands; only 78 of these sub-bands are used in order to comply with frequency regulations concerning radio amateur networks (compliance with 40m, 30m, 20m, and 17m amateur bands).

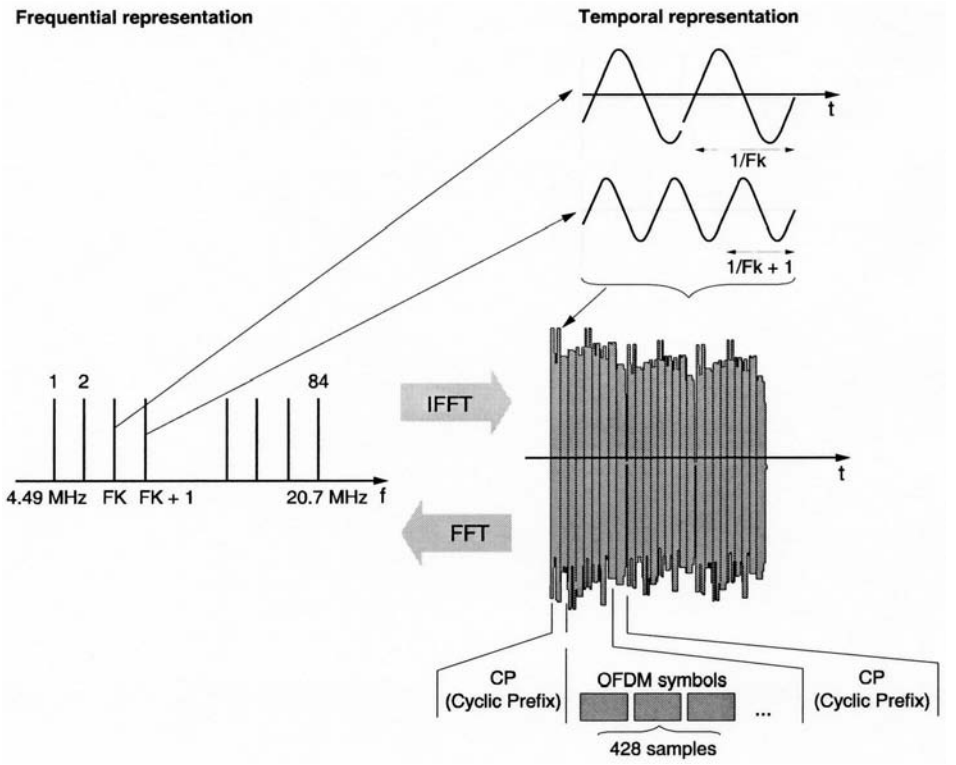

Figure 5.5 Temporal and frequential representation of OFDM frequency bands

Each frequency sub-band conveys OFDM frames comprising two main parts:

- The CP (Cyclic Prefix) is used for the temporal delimitation of the part conveying the data.
- The data frame consists of OFDM symbols, each of which consists of 428 samples.

The OFDM blocks of the HomePlug frame consist of 20 or 24 symbols. Those of the ROBO frame only comprise 40 symbols.

Figure 5.6 gives details on an OFDM symbol and the respective times for its various parts: 8.4 μs for HomePlug 1.0 and 40.96 μs for HomePlug AV.

The long data frame is itself composed of 20 to 120 OFDM blocks forming the data of the data link layer and the service blocks.

The OFDM symbols are modulated in each frequency sub-band with phase modulation according to the quality of the link between PLC devices.

OFDM Transmission Schemes

Unlike single-carrier transmission schemes, OFDM transmission schemes are used to share the complexity of power equalization for the signal transmitted between the sender and the receiver. This ensures simple and cost-effective implementation of PLC receivers.

The other advantages of OFDM transmission schemes are the following:

- Efficient use of the frequency band unlike conventional frequency-division multiplexing techniques. The various channels overlap in spectral terms while remaining fully orthogonal.
- Digital equalization and simple and optimum decoding thanks to the use of guard spaces even if accompanied by a lower data rate. Used in conjunction with convolutional codes, Viterbi codes, and block codes (Reed-Solomon codes), this technique proves to be highly efficient.
- Robustness to burst noise thanks to a multicarrier technique. Each carrier is affected by a noise independent from the other carriers. In the single-carrier technique, the

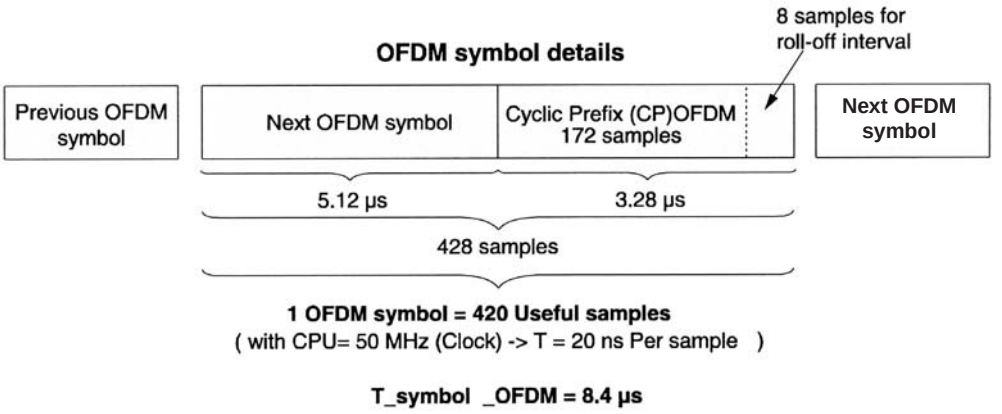
OFDM symbol details
8 samples for roll-off interval
Previous OFDM symbol
Next OFDM symbol
Cyclic Prefix (CP)OFDM 172 samples
Next OFDM symbol
5.12 µs
3.28 µs
428 samples
1 OFDM symbol = 420 Useful samples
(with CPU= 50 MHz (Clock) -> T = 20 ns Per sample)
T_symbol _OFDM = 8.4 µs

Figure 5.6 OFDM symbol details

noise can affect some symbols. In the OFDM technique, symbol losses in a carrier do not affect other carriers.

- High bit rate allocation flexibility for each user or each carrier. Each carrier can be encoded independently from the other ones according to the quality of the physical links and to the best suited modulation techniques.
- Improvement of the transmission channel preliminary estimate. Training frames used to identify the transmission channel capacities in the frequency domain are used by the OFDM techniques.

Figure 5.7 gives an overview of the OFDM symbols in each channel (frequency sub-band).

The HomePlug 1.0 frame uses several modulation, frequency division, and error correction techniques, which constitute a data processing set for each PLC device between the physical analog interface and the Ethernet interface of the RJ-45 type.

Frequency Band Use for HomePlug AV Devices

Technical evolutions in the field of signal processing in media with high interference led the developers of PLC solutions within the HomePlug industrial consortium to make maximum use of the authorized 1-30 MHz frequency band in order to achieve transmission speeds around 200 Mbit/s.

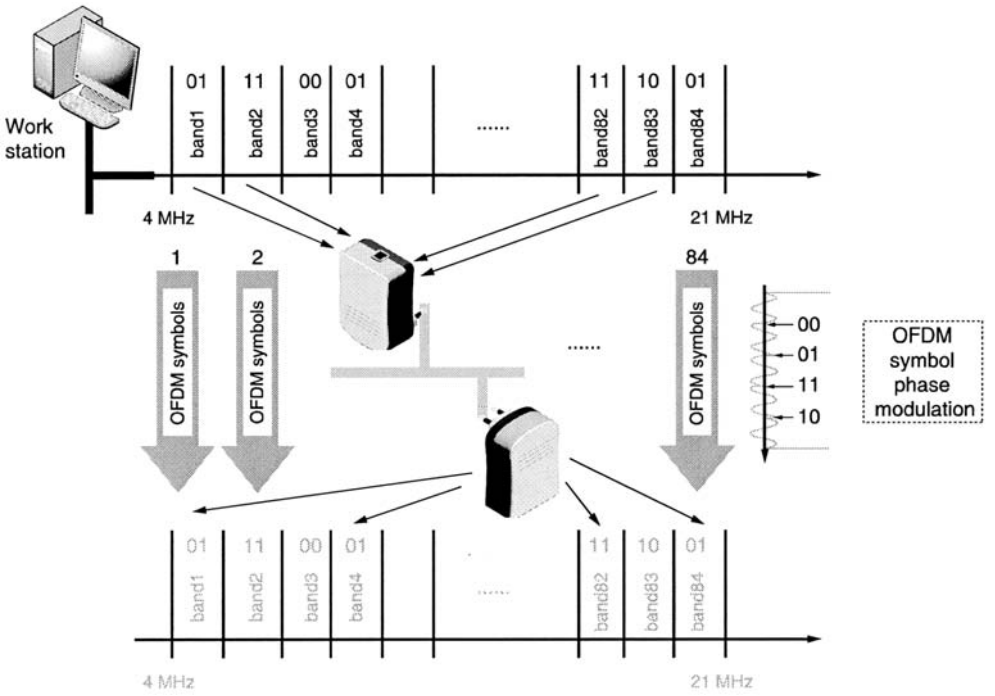

Figure 5.7 Distribution of OFDM symbols over frequency bands

The 917 frequency sub-bands at the physical layer are used by HomePlug AV. Each band then uses OFDM symbols in order to encode the data in an orthogonal manner in the frequency domain. Therefore, the bands are independent in terms of frequency and do not interfere with each other.

In each frequency band, the data and its OFDM symbols are encoded using a turbo convolutional code. The modulation is then carried out; it is potentially different for each frequency band (see Figure 5.8).

This modulation can range from the BPSK type, which encodes 1 bit for each symbol and frequency band, to the 1024-QAM type, which encodes 10 bits for each symbol and frequency band.

Functional Blocks

Therefore, a PLC device consists of various signal processing electronic elements. Each electronic element has a precise function in the signal processing chain that conveys data from the interface connected to an Ethernet network or from the interface connected to an electrical network.

Figure 5.9 illustrates the functional blocks used to send and receive HomePlug 1.0 frames between the various network PLC devices with adaptations relating to the quality of the electrical transmission channel.

These adaptations must be made as efficiently as possible in order to achieve optimized performance for the upper protocol layers and the various terminals connected to the Ethernet interfaces of each PLC device.

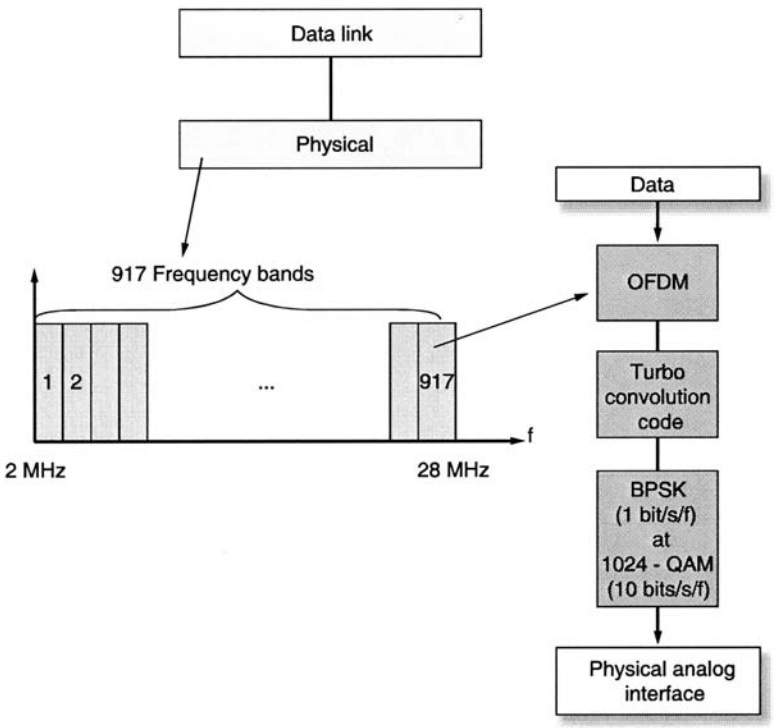

Figure 5.8 Details on frequency band use in HomePlug AV

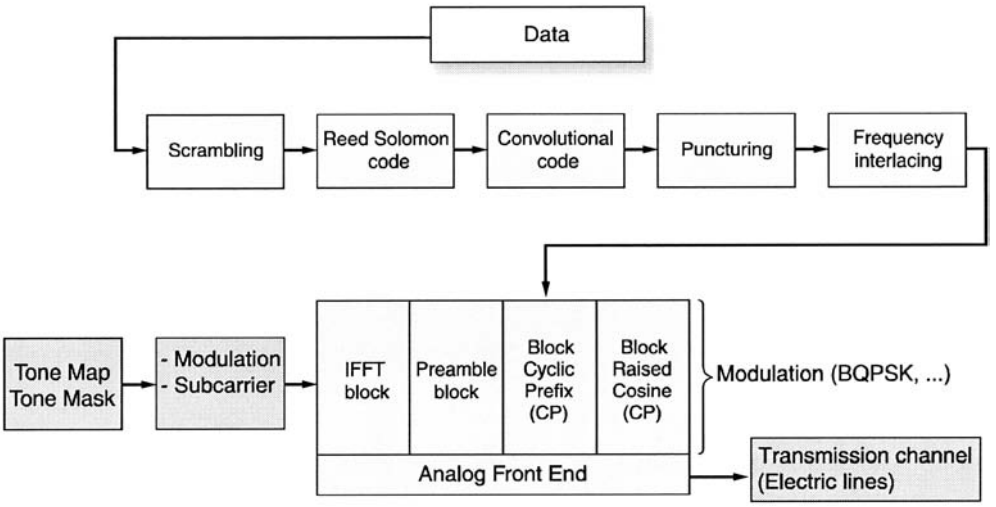

Figure 5.9 Functional blocks for data signal processing in HomePlug 1.0

Differences Between HomePlug Frames and 802.11b Frames

From a functional point of view, there are a few differences between the various parts of the HomePlug 1.0 frames and the IEEE 802.11b frames.

The main difference concerns the MAC encapsulation of the PLC technologies. MAC type data are defined in it in complete frames, whereas the IEEE 802.11 frames must implement the LLC layer and a more complex MAC frame reconstitution process.

Figure 5.10 illustrates, in the boxes with arrows, the fields that differ between the two standards since the 802.11 standard uses a slightly different contention technique and additional interframe spaces.

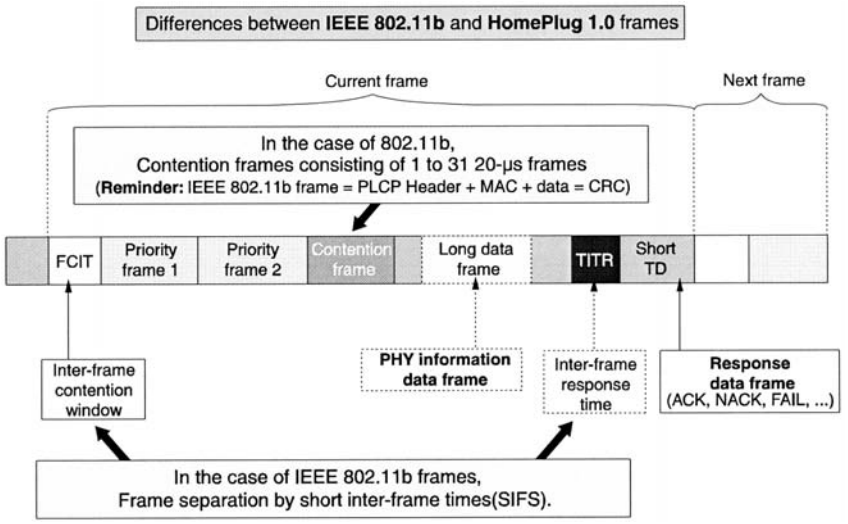
Differences between IEEE 802.11b and HomePlug 1.0 frames
Current frame
Next frame
In the case of 802.11b,
Contention frames consisting of 1 to 31 20-µs frames
(Reminder: IEEE 802.11b frame = PLCP Header + MAC + data = CRC)
FCIT
Priority frame 1
Priority frame 2
Contention frame
Long data frame
TITR
Short TD
Inter-frame contention window
PHY information data frame
Inter-frame response time
Response data frame
(ACK, NACK, FAIL, ...)
In the case of IEEE 802.11b frames,
Frame separation by short inter-frame times(SIFS).

Figure 5.10 Differences between HomePlug 1.0 frames and IEEE 802.11b frames

The PLC Physical Frame

In HomePlug 1.0, the physical layer frames, or PHY PPDU (physical protocol data unit) are strongly related to the MAC layer frames, as some MAC layer information is available at the PHY layer level.

There are two PPDU types at the physical layer level: a long PPDU and a short PPDU, as well as a number of elements delimiting these PPDU or allowing sufficient spacing between them so that the stations have the time to transmit or receive the frames.

The various elements of the HomePlug 1.0 physical frames are the following:

- Three delimiters:
  - SOF (start of frame), which is used to delimit the start of the frame;
  - EOF (end of frame), which is used to delimit the end of the frame;
  - Short PPDU, which is the response frame sent back by the destination station to indicate acknowledgment of the transmitted data.
- Two time intervals between two frame transmissions:
  - CIFS (contention distributed interframe spacing), which is the end of frame gap before the end of frame delimiter.
  - RIFS (response interframe spacing), which is the time interval during which a station waits for a response from the destination station.
- Long PPDU, which contains the data frames.

Figure 5.11 illustrates all the parts forming a PLC physical frame in HomePlug 1.0 and Turbo with the long frame containing the data of the upper layers, the interframe gap used to delimit the frames on the physical medium, and the short frame used to manage the responses from the PLC devices and optimize the communication times over the medium.

The physical level long frames, also called PLCP PPDU (physical level common protocol PPDU), are nothing else than blocks of bits sent over the physical layer.

These long frames, also called long PPDU, comprise six parts: preamble, frame check, header, frame body, padding bits, and FCS.

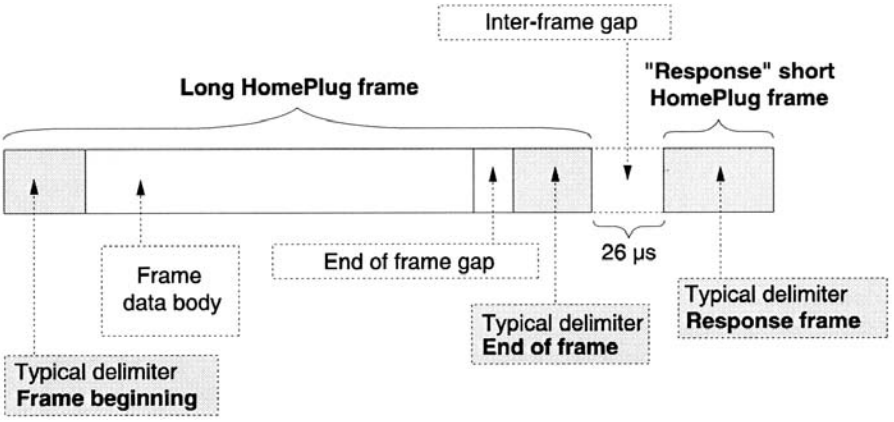

Figure 5.11 Elements of HomePlug 1.0 physical frames

- The preamble included in the SOF indicates the timestamps of the MAC type frames.
- FC (Frame Check) is used to check the frame. The frame consists of four OFDM symbols that are highly resistant to the noise on the transmission channel and use a turbocode convolutional code. This code is widely used for signal processing in HomePlug AV. These four symbols must be transmitted over the transmission channel in order to make it possible for the destination station to know the state of the link and the number of errors in the transmitted data.
- The header contains various information concerning in particular the connection bit rate, which can vary according to the signal quality.
- The frame body contains information from the MAC layer just above. This information is also called MPDU (MAC protocol data unit).
- The padding bits are used to fill the frame if a minimum frame size cannot be achieved with the useful data.
- FCS (frame check sequence) is used to check the integrity of the data contained in the frame body.

All the HomePlug 1.0 frame times without priority and contention headers are estimated to be 1.5 ms, including the frame body, which includes 160 OFDM symbols lasting 1.328 ms.

Figure 5.12 illustrates the constituent elements of the long frame in HomePlug 1.0 and Turbo. This long frame globally consists of three parts: the start of frame, used to identify a long frame on the network; the data (in which the frame body with the data of the upper layers is found); and the end of frame, used to identify end of frame and therefore to indicate to the PLC devices that these devices can send the next frames.

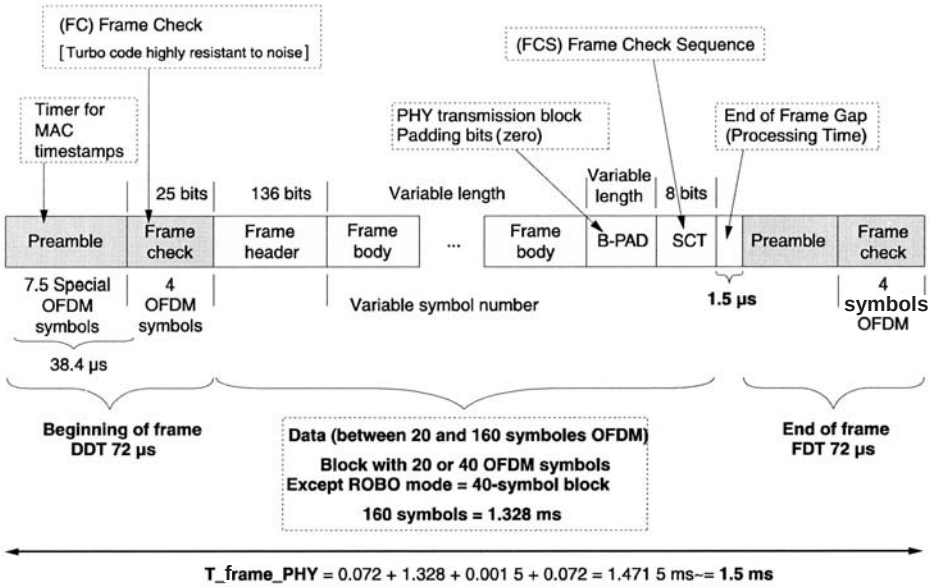

Figure 5.12 HomePlug 1.0 long frame structure

Physical Frame Start Delimiter

The start delimiter contains two parts, the preamble and FC:

- The preamble contains the frame sending time stamp.
- FC (frame check) contains several fields: a contention check field, used to check the contention level of the transmitted frames; a field indicating the delimiter type; a variable field, which itself comprises two fields that are of particular importance for PLC communications (the tone map, which stores the states of the links between PLC stations and the size of the following data frame) and a frame check sequence. A CRC (cyclic redundancy check) is used in the latter field to check the frame integrity check sequence (see Figure 5.13).

Physical Frame Data Body

The physical frame data body is illustrated in Figure 5.14. It comprises a MDPU encapsulated into the PPDU. The MPDU comprises the EB (block header), PAD (padding bits) (if the data does not completely fill the data part), and the SCB (bit check sequence) fields. An ICV (integrity check value) is used by the SCB field to check the integrity of the data forming the data body.

Physical Frame End Delimiter

The physical frame ends with an end delimiter, which consists of a preamble and of a frame check field.

The frame check field consists of the four following fields (see Figure 5.15):

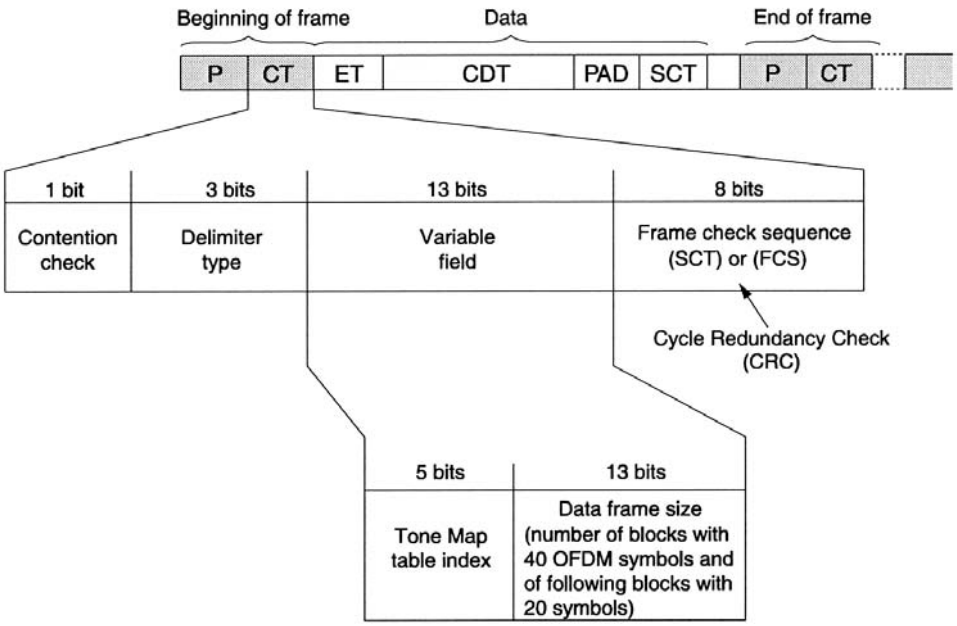

Figure 5.13 Start of frame header of physical frame

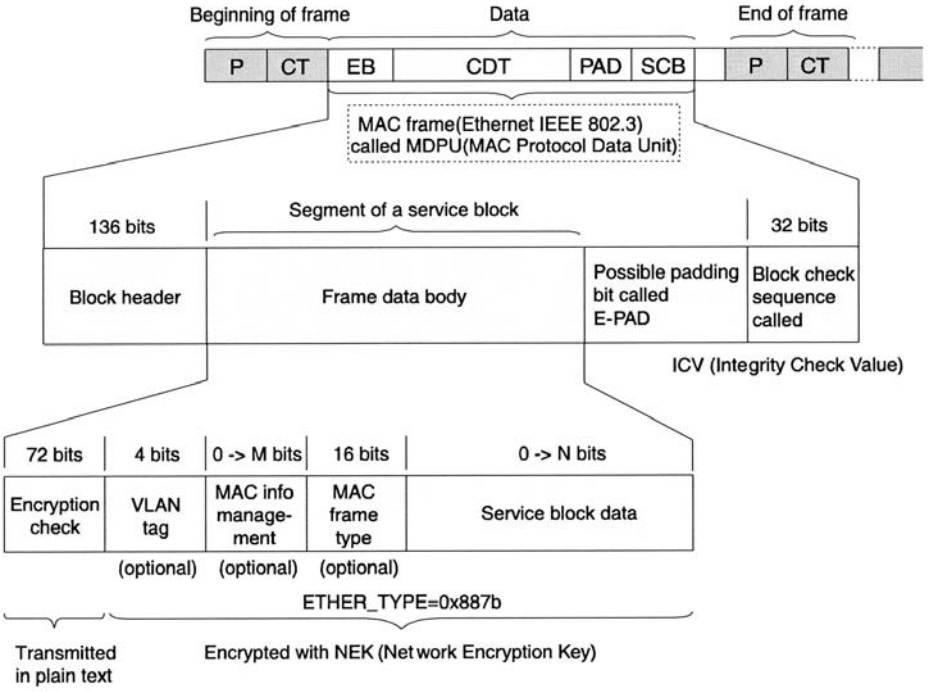

Figure 5.14 Physical frame data body

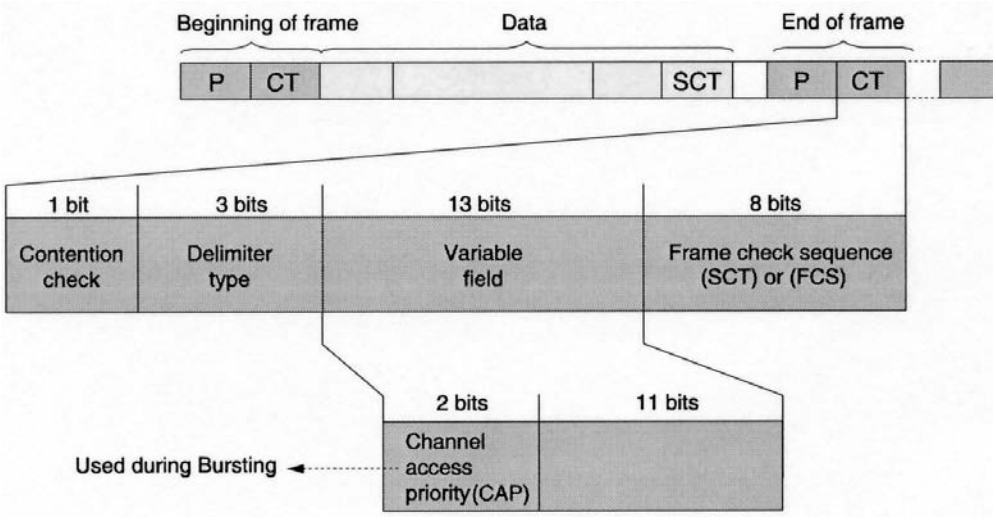

Figure 5.15 End of frame fields of physical frame

- Contention check used to check the state of the contention periods between frames.
- Delimiter type specifying whether the delimiter is at the beginning or at the end of the frame.

- Variable field specific to this delimiter, which contains the priority level of the PLC station (indicated by the CAP parameter).
- FCS, which uses a 16-bit CRC for the frame integrity check. The FCS is calculated both on the frame header and body. The techniques used in FCS are usually defined in the main standards on frame transport over a link.

MAC Layer Frames

The MAC (medium access control) layer frames, situated just above the physical layer, allow a link with the layers of the upper levels.

As indicated before, the PLC technology can be viewed as a MAC encapsulation since MPDU frames are encapsulated into long PPDUs. Likewise, all data coming from layers above the MAC layer is encapsulated into the MAC frame.

MAC HomePlug 1.0 Frames

In the case of HomePlug 1.0, the encapsulation of the IEEE 802.3 or MPDU (MAC protocol data unit) frame is included in the frame body of the PLC frame between the start and end delimiters.

The Ethernet HomePlug 1.0 frames can be easily identified on an Ethernet network since, for all of them, the hexadecimal 0x887b value is indicated in the MAC ETHERTYPE frame type field. This parameter is used to create applications at the data link layer level dedicated to HomePlug PLC technologies. In the case of HomePlug AV, the value of the ETHERTYPE field is 0x88e1.

In addition to the 72-bit encryption check, the data body is encrypted with the NEK (network encryption key) exchanged between the various PLC stations of the network.

The MPDU form what is called a service block (BS). If the BS exceeds the limit size of the MAC frames (1,500 bytes), the BS is fragmented into segments sent in sequence by the source stations. The MPDU are then subjected to a fragmentation-reassembly sequence during the transmission and receipt by the various PLC stations of the network.

Each segment of a MPDU is numbered and sequenced to be reassembled by the destination station.

MAC Header Format

The MAC frame begins with a rather complex header containing three fields of total length 17 bytes as illustrated in Figure 5.16.

Block Check Field

The first field of the header comprises 40 bits subdivided into eight subfields. The purpose of this field is to convey check information that the MAC layer requires.

Figure 5.16 illustrates the frame check field and its division into subfields. The purpose of the various subfields is the following:

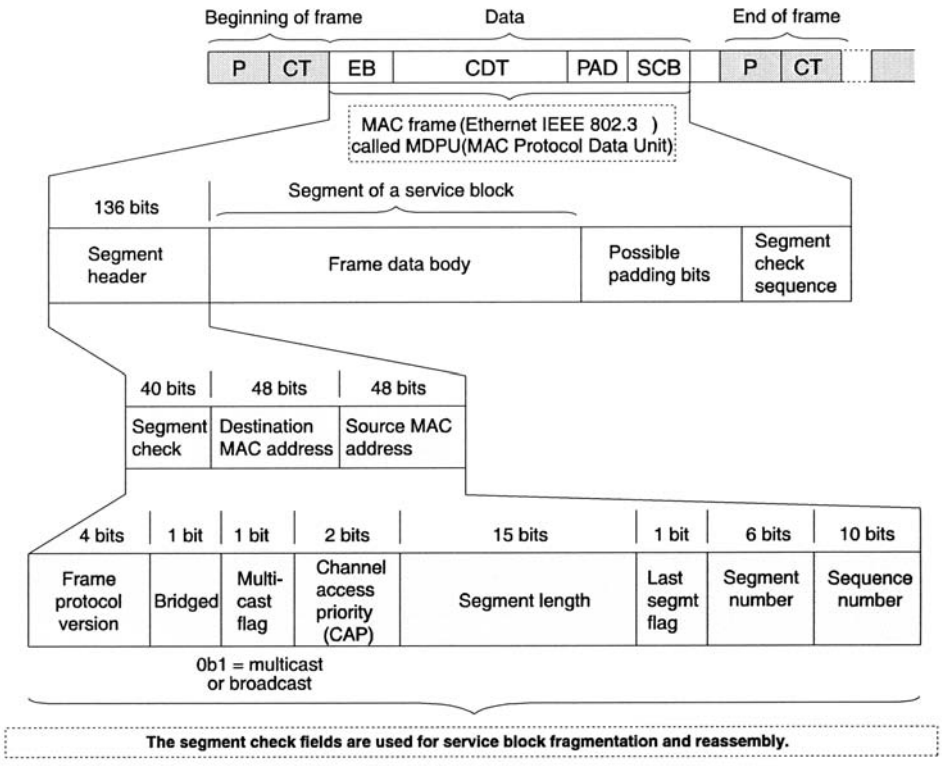

Figure 5.16 HomePlug 1.0 MAC frame header

- *Protocol version*. Defines the value of the protocol used. This value is reserved and will only be used during a standard evolution.
- *Bridged*. Indicates whether the PLC station transmitting the data is in bridge mode and has the potential for relaying the frames to other network stations.
- *MCF (multicast flag)*. Indicates whether the frames are sent in multicast or broadcast mode by setting this value to 0b1.
- *CAP (channel access priority)*. Reuses the priority level of the source station in comparison with the other stations of the PLC network.
- *Segment length*. Used to find out the data length of the transmitted segment.
- *LSF (last flag segment)*. Used to find out, if the value is set to 0b1, that this segment is the last BS segment.
- *Segment number*. Indicates the fragmentation and reassembly order for the various BS segments.
- *Segment sequence number*. This number, set to 0, is assigned to each frame and incremented by 1 steps for all the other transmitted frames. If a frame is fragmented, all the segments of this frame have the same sequence number.

Address Fields

In HomePlug, all the address fields have a 6-byte length and the same format as the addresses defined in the IEEE 802.3 standard.

The 48-bit address consists of the four following parts:

- *Individual/Group (I/G)*. The first bit indicates whether the address is an individual (1) or group (0) address.
- *Universal/Local (U/L)*. The second bit indicates whether the address is a local (1) or universal (0) address. If this is a local address, the following 46 bits are locally defined.
- *Organizationally unique identifier*. The number assigned by IEEE corresponding to the 22 bits following the I/G and U/L bits.
- *Serial number*. The last three bytes, i.e., 24 bits, correspond to the serial number generally defined by the manufacturer.

Hexadecimal Format

The hexadecimal writing, or base 16 numbering system, of the MAC address is generally preferred to binary writing.

The MAC addresses consist of two distinct address families: individual addresses addressing a single station on the network, and group addresses addressing several stations on the network. In the latter case, the MAC address represents a group of stations.

There are two types of group addresses:

- *Broadcast address*. This address is associated with a group of stations consisting of all the network stations. Information can be sent to all the network stations using a broadcast address. A broadcast address always has a 48-bit format; all the bits are set to 1.
- *Multicast address*. Like for the broadcast address, this address is associated with a group of stations but in finite number. This type of address always begins with the first 24 bits of the MAC 48-bit address equal to 01:00:5E (hexadecimal).

A MAC 802.3 frame like that used in HomePlug contains the two following address fields:

- *DA (destination address)*. The address to which the frame or segment is transmitted. The DA address can be an individual or group address.
- *SA (source address)*. The address that has transmitted the frame or the segment. The SA address is always an individual address.

Format of an Encrypted MAC Frame

The IEEE 802.3 standard enables the encryption of a frame to go across the power line medium so that no user can decrypt the information.

In practice, as illustrated in Figure 5.17, a frame is only partially encrypted. The frame is encrypted using the two following fields:

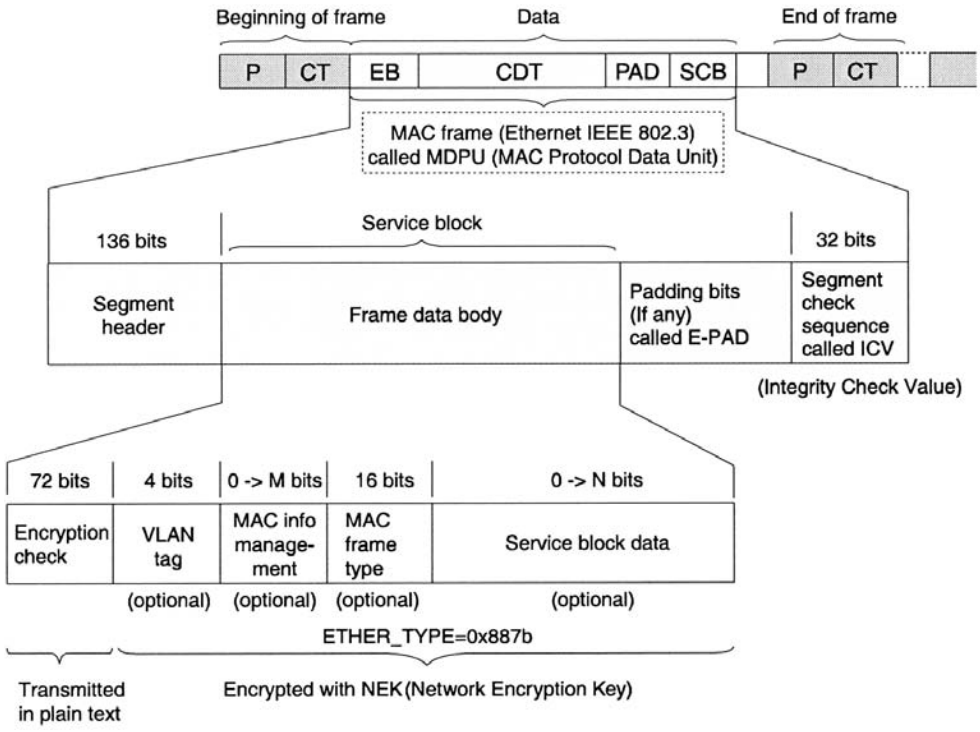

Figure 5.17 Encrypted HomePlug 1.0 MAC frame details

- *IV (initialization vector)*. Initialization vector with a block of bits concatenated with the block of main data used for decrypting frames. The IV is reinitialized after each use. The combination of IV and data creates a unique encryption key.
- *EKS (encryption key select)*. Index used to retrieve the NEK used for frame decryption.

Format of Control and Management Frames

The purpose of control and management frames is to send supervision information and commands to the network elements that need them in order to operate.

As illustrated in Figure 5.18, information concerning the frame length and response expected by the source station is used to manage and control the frames (see Chapter 3).

Some manufacturers of PLC products implement specific MAC layers to make it easier to manage and control the networks.

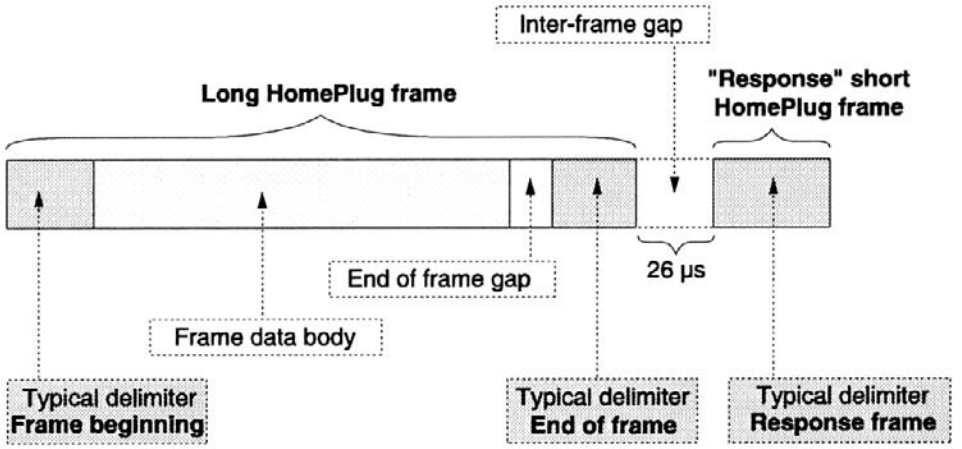

Figure 5.18 Control and management fields of PLC frames

PART II

PLC in Practice

The first part of the book introduced the architecture of PLC networks and explained how they operate from a theoretical point of view. This second part, focused on practice, details the rules to follow when installing such networks by putting the emphasis on the new application possibilities brought about by concepts relating to data broadcasting over an electrical network as well as on the electrical constraints and choosing, installing, and configuring the devices.

The simplicity and practicality of PLC networks means they can be developed quickly, which is sustained with the appearance of new PLC technology versions resulting in new applications and the emergence of the IEEE 1901 standard for PLCs in the very near future.

From an applications point of view, PLC networks do not bring about particular changes, and usual applications, particularly voice and video, are used. However, using an electrical network to convey high rate data has brought about unexpected applications such as conveying data in a motor vehicle or using PLC as the backbone of a Wi-Fi network.

We are still at the early stages of these new techniques, and the applications will evolve with time to integrate more user friendliness, simplicity, and more functions in particular, which is undoubtedly the most important element as far as the user is concerned.

Although the PLC philosophy seems simple at first, this is not the same when focusing on its technical specificities. With regard to electronics, for example, the notions of electrical network topology and interference are essential features to be considered when installing a PLC network. In addition, it is important to differentiate useful throughput notions from theoretical rate notions. This rate corresponds to the network transmission speed. The usable rate is lower because of the mechanisms implemented by the network protocols of the various layers (physical, data link, network, transport, and so forth). These mechanisms were discussed in detail in Chapters 3 and 5.

The basic device of a PLC network has highly evolved over the few last years. Initially, only terminals in the form of bulky desktop packages that were relatively unsuited to the users' requirements were available. Now, the devices have all kinds of configurations with several interfaces and many integrated network functionalities (router, modem, Wi-Fi access point, switch, and so forth) so that custom-made configurations adapted to the user's needs can be set up.

Configuring a Wi-Fi network starts with configuring the terminal and therefore the PLC adapter. The configuration details in this section are for Windows XP, Linux, and FreeBSD operating systems. Once the terminal is configured, the instal-

lation phase takes place. A number of constraints must be respected in this phase, such as the electrical network topology, security, and performance.

By following the advice and configuration procedures explained step by step throughout the chapters of this section, the reader will then be capable of installing and configuring without assistance a PLC network in the best possible conditions.

We'll conclude this section and the book by introducing the future standards on PLC networks that, in the near future, will form the basic elements of the Internet for both home and professional use, making it easier to develop home automation. Remember that home automation is based on data exchanges within a house or a building.

CHAPTER 6

Applications

Many prospective studies show that, in a few years from now, Ninety percent of the networked terminals will not be computers. This prospect shows that many electrical and electronic devices of any type in many fields (industry, hospitals, home automation, electronics, digital arts, and so forth) will be fitted with an RJ-45 network interface used for connecting to a local area Ethernet network.

The last few years have witnessed the predominance of two major standards on networks—Ethernet and IP. From these observations, it is logical to think that the communication networks between devices will mainly develop over the most convenient and reliable communication media. From this perspective, PLCs will undoubtedly be major players due to the extent of the electrical network (outlet networks, light network, and so forth) to provide the various devices with the most recent functionalities of networked communications.

The PLC networks bring about new advantages for the network world; the most important one is undoubtedly how easy it is to use, since the user just has to use the outlets of the building to build a computer network.

Once installed, this network provides sufficient data rates for real-time and multimedia applications. In addition, it can act as the backbone of a Wi-Fi network. The PLC network then ideally completes Wi-Fi; this makes it possible to extend its coverage and to obtain the best offered by this technology.

Voice, Video, and Multimedia

Voice and video are real-time applications that are not easily implemented in asynchronous networks such as PLC. However, they probably represent a part of the future of these networks as an extension of the telephone application.

In 2005, the conventional telephony around PABX and its distribution to telephone sets started to be replaced by telephony over IP in a PLC environment. Now, since the beginning of 2007, PLC networks have been broadcasting television channels and handling videoconferencing applications between users. As for the multimedia application, it has rapidly become a major criterion for choosing PLC technology, in particular among companies.

Telephony over PLC

The bit rate is not a problem in itself to convey telephone speech, since it can be as low as 5.6 Kbit/s and that such a value is supported by PLC networks to a large extent.

On the contrary, since telephony application is interactive, more than 300 ms must not elapse between the moment when the information is sent by a user and the moment when it is received by the recipient. If this is a symmetrical network, the maximum round-trip time must therefore not exceed 300 ms. This is the maximum permitted value for an application with human interaction.

Synchronization represents the second constraint when conveying telephone speech. The information must be available to the receiver at precise times. In particular, the bytes originating from the digitization must be delivered at fully determined synchronization times. For example, if the compression generates a 8-Kbit/s flow, this involves synchronizing every microsecond. Therefore, a byte must be delivered to the receiver on each microsecond. If speech is not compressed, a 64-Kbit/s channel is synchronized every 125 μs.

The third main characteristic of PLC telephony is the use of the VoIP (voice over IP) technique. The speech bytes are routed in IP packets and use the same network resources as the packets routing other applications. Therefore, telephony over PLC is integrated into the conventional framework of speech over IP.

Figure 6.1 illustrates the synchronization constraint at the remote telephone level. Although the packets are regularly transmitted by the sender, they are received at irregular intervals; because of this, delivering speech bytes to the receiver at precise times is rather difficult. This irregularity on receipt is due to the crossing of the PLC network, which makes the speech packets arrive at random times.

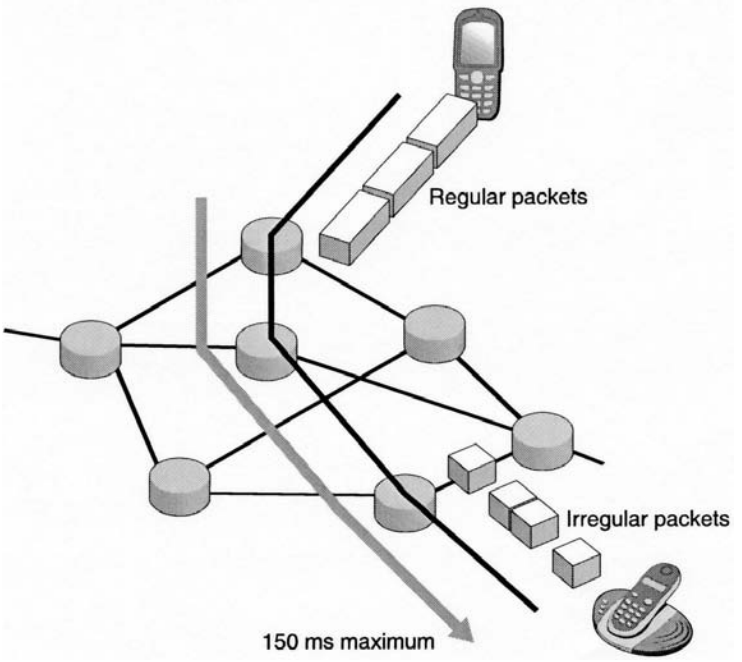

Figure 6.1 Telephone communication constraints

The access method used to obtain the right to transmit to the access point, the CSMA/CA (carrier sense multiple access/collision avoidance), makes the PLC network crossing time random. In addition, to reach the recipient, the packets must cross wider networks and go via intermediate transfer nodes that are also crossed randomly.

Speech Packetization and Depacketization

Let's suppose that speech is compressed to 8 Kbit/s, which is the most usual standard in telephony over IP environments.

The telephony bytes must be packetized into an IP packet which is itself encapsulated into an Ethernet frame or, to be more precise, into a PLC frame for transmission over the electrical network.

The synchronization takes place on each microsecond at a speed of 8 Kbit/s. If n represents the number of bytes that can be used in a PLC frame, the filling time is n ´ 1 ms. Since the minimum length of the PLC frame is 64 bytes, the packetization requires 64 ms.

Depacketization does not actually require additional time since it is carried out at the same time as packetization. Therefore, the packetization-depacketization time is equal to at least 64 ms. In fact, the tendency is to add the packetization and depacketization time to take account of the latency found in most packetizers-depacketizers.

It is acceptable for this 64-ms time to remain below the 150-ms outgoing path. However, this 64-ms value may prove to be too high if the packet has to go across networks other than the PLC network or if the packetizers-depacketizers are much too slow. This is the reason why speech packets are only filled with 16 byte speech and the remainder is completed by padding bytes to achieve the minimum frame size. The packetization-depacketization time can still be on the order of 16 ms with these 16 bytes.

Actual Rate

The actual rate over the network is in fact much higher than 8 Kbit/s since the packet contains a lot of additional information like headers and padding bytes. It is considered that the actual rate over a PLC network or any other packet transfer network is around 60 to 70 Kbit/s using the IPv4 standard and after encapsulation into an Ethernet frame.

If the IPv6 standard is used, the supervision fields are even bigger and we consider that a speech channel exceeds 100 Kbit/s.

The time that the coder-decoder (codec) requires to digitize the signal from an analog signal or vice versa can be estimated to be around 5 ms. Therefore, 26 ms are obtained for coding, decoding, and packetization-depacketization. The total allowable transport time therefore becomes 124 ms (maximum transport time of 150 ms, as indicated at the beginning of this section, minus 26 ms for the various times). The technique for MAC access to the PLC network is included in this transport time.

Transit Time

In PLC, the waiting time to access the power line medium can be relatively long. If, for example, five clients are connected to the same electrical network by using 1,500-byte frames and integrating access times related to CSMA/CA, a waiting time on the order of 10 ms, or even more, is obtained. If the telephone speech is supposedly intended for another employee of the same company connected to a PLC network, about ten milliseconds for access to the network must be added again.

Altogether, the transit time remains around 100 ms assuming that the traffic is relatively high but without collisions. This time makes it possible to transport telephone speech under good conditions over a PLC network.

With the exception of the HomePlug AV standard and developments in progress by competitors, because priorities are not managed by the current PLC generation, the packets of other users circulate with the same priority, even if they convey data that is not of immediate interest. For example, the packets of a client working under a peer-to-peer (P2P) application and recovering a video file with several gigabytes randomly circulate ahead of the packets a user on the phone. This is the reason why drastically limiting the number of users or the global traffic is essential for the current PLC generation. The next HomePlug AV PLC generation will be capable of managing the priorities of telephony and video packets, thus ensuring the quality of service over the data network.

If the number of users exceeds ten, or if the useful bit rate exceeds 5 Mbit/s, transporting a telephone speech successfully using a Homeplug 1.0 PLC network cannot be guaranteed, i.e., with the necessary quality of service. In this case, another technique must be used to assign priorities to the packets carrying telephone speech.

Differentiating IP Packets

Two solutions can be deployed in the short term to implement this differentiation between packets passing through PLC:

- A technique for IP packet control at the IP protocol level. In this case, the PLC network manager slows down the incoming acknowledgments of nonpriority packets delivered by the receiving stations in such a way that these streams are maintained in a slow-start condition, in which the sending stations can only send a few packets and must wait for acknowledgments.
- Use the HomePlug AV standard, which was released in 2007. This standard determines priorities at the MAC layer level. In this case, assigning the highest level priority to the telephone terminals is enough.

The second solution is clearly the best one, as it can be applied at the lowest level of the architecture and clearly favors telephone speech streams. The other solution is more artificial, as it consists of restricting non-priority streams without estimating the actual bandwidth requirements of clients having priority of the telephone speech type.

Figure 6.2 illustrates the various components crossed when transporting telephone speech within a broader framework than a simple conversation from a termi-

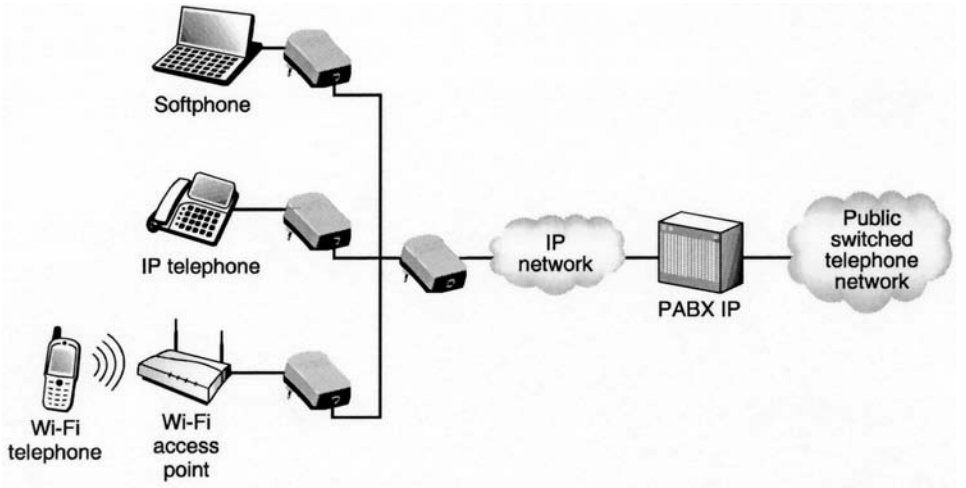

Figure 6.2 Devices crossed by a PLC digital speech stream

nal to another one in the same PLC network. After going across the outgoing PLC network, the stream of telephone packets is routed in a fixed IP network, which can be an operator network, then goes via a dedicated gateway, PABX IP, before crossing the conventional telephone infrastructure. PABX IP converts IP addresses into telephone addresses and carries out the necessary code conversions of a compressed stream to a 64-Kbit/s operator telephone stream.

The Asterisk software is typically used to create an IPBX (PABX), which manages the local IP calls and the outgoing calls to the STN (switched telecommunications network) at the server level.

Hi-Fi Quality Telephony

PLCs are used to carry speech of much higher quality than the conventional telephone voice. Indeed, since they do not have constraints on the bit rate, they can absorb a high bandwidth likely to carry hi-fi or almost hi-fi quality.

Suppose you have a 512 Kbit/s speech compressed to 64 Kbit/s. To fill the 64 bytes with telephone data, only 8 ms are necessary. Globally, the rate of the IP packet stream is the same as before but, failing it filling with padding bytes, it only contains useful bytes. Therefore, speech with much higher quality can be transported at the same actual rate.

This technique is still not widely used since the telephone devices are not always compatible with such quality. The compatibility could be found by using a microcomputer with a sound board. Unfortunately, this solution does not prove to be better, since the sound boards on the market are very slow and require a processing time of about 50 milliseconds that, when two devices must be crossed (that of the sender and of the receiver), makes the transit time unacceptable.

In any case this example shows that an interesting extension of telephony over PLCs could be high quality telephony.

Video

Video is another application that should develop in the future in PLC networks. This application especially requires a high rate that becomes accessible in PLC environments.

Depending on the video application type being considered, the time constraint is more or less strong. The two main cases, streaming video and videoconferencing, are examined below.

Streaming

With streaming without a return channel, like video on demand (VoD) and television, between the time when the video stream is sent from the source and the time when this video is played on the screen, a rather long time can elapse in the order of several seconds up to about fifteen seconds. The viewer does not necessarily have the feeling that the video source sends correctly before he or she views the images.

The single constraint to be observed for these applications is the waiting time at the beginning of the video. It is rather irritating to have to wait while the application initializes itself whenever the channel is changed due to resynchronization at the receiver level. The purpose of streaming is to leave some advance for the packet stream to reach the receiver and to have enough packets in memory in the receiver so that there is no interruption in the packet delivery to the client. This constraint is illustrated in Figure 6.3.

The video can come from an analog signal that is digitized then compressed, or from a digital signal which is compressed already. It can be highly compressed or may require a high rate; this depends on the network possibilities and the computing power of the emitters and receivers.

The higher the bit rate and the lower the compression, the higher the image quality. This requirement concerning the rate is a major feature of the transmission of a video image. This characteristic poses no particular problems for PLC networks as long as the network is not saturated. Let's first analyze the necessary rates for routing a video channel.

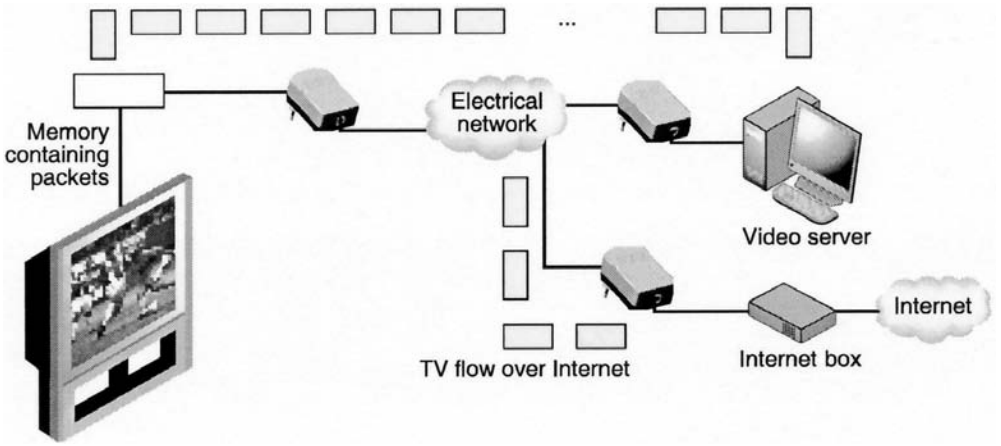

Figure 6.3 Streaming video application over a PLC network

Necessary Rates for Video Routing

The video devices mainly use the most recent MPEG standards. DVB (digital video broadcasting) is also widely used.

MPEG uses inter- and intraframe compression algorithms. The rate can be as low as 1.5 Mbit/s for television quality with very few losses in comparison with the original image. New developments improved the image quality with bit rates for MPEG-2 of around 4 Mbit/s. An even higher compression can be envisaged with the MPEG-4 standard by including, where applicable, the elements that are necessary for reconstructing the image at the other end.

The difficulty with broadcast television resides in the fact that the bit rate is very variable over time and must adapt itself to the transport network. The algorithms more or less compress the information according to the time and resources available on the medium. If the network is almost fully available, the image quality can be highly improved. If, on the contrary, it is congested by miscellaneous information coming from various sources, a degradation of the video transmission must be envisaged if the quality of service demanded by the user allows this. A control mechanism is essential to fully optimize the application transfer.

High-definition digital television (HDDTV) requires a bit rate of around 5 to 10 Mbit/s according to the quality demanded by the user. This 5 Mbit/s rate is almost too big to be supported by the HomePlug 1.0 and Turbo networks. With HomePlug AV (40 Mbit/s), only two users have access to the service.

However, HDDTV broadcasting over PLC networks is now available but is restricted to a maximum of ten users.

Capacity Problems

A PLC network must be capable of providing connections enabling a video application to use the optimum bit rate while allowing it to maintain an acceptable quality of service.

Let's first examine the difficulties raised by capacity. For telephone speech, there is no problem since, once compressed, the stream is 8 Kbits/s, even 5.6 Kbits/s. On the contrary, for video, the capacity required for a MPEG-2 television quality image varies between 2 and 8 Mbits/s. With the MPEG-4 generation, it goes down to 1 Mbit/s. In any case, it is currently 2 Mbits/s. These values can drop to some hundreds of kilobits per second by reducing the video quality.

If the bit rate of a HomePlug 1.0 network proves insufficient to broadcast good quality video, the bit rate of a HomePlug Turbo or HomePlug AV network should suffice. Since the useful bit rate is around 10 Mbit/s and 40 Mbit/s for these two technologies, having a rough estimate of its own stream and of the stream of other applications on the network is enough not to exceed these values.

Giving streaming flows a higher priority level is possible by using the same priority techniques as in the transfer of the telephone speech. In this case, there are no longer bit rate problems by using the HomePlug Turbo and AV networks.

If the capacity is adequate, i.e., if the number of users is small enough with respect to the capacity required, or if a priority scheme is implemented, the second problem to solve concerns compliance with the latency for byte resynchronization. This is the reason why the latency is generally of the order of several seconds, even

several tens of seconds if this is necessary. In this case, once the streaming application is started, the first image only appears at the end of this latency.

Visioconferencing and Videoconferencing

Visioconferencing and videoconferencing are applications with human interactivity, which requires a 150-ms latency. As explained previously, the data resynchronization process must be observed to reconstitute the isochronous application to the receiver. For this purpose, a quality of service must be associated with transporting these applications.

The difference between the two application categories comes from the quality of the broadcast image.

In visioconferencing, the image can be black and white and jerky due to the number of images per second being lower than normal. A low resolution screen can be used by this application in order to reduce the bit rate. These characteristics only require a transport capacity lower than 100 kilobits per second.

Videoconferencing requires a much higher bit rate (several megabits per second) to obtain an image quality comparable to that of television. To obtain cinema quality, about 50 megabits per second must be achieved, which cannot be envisaged within the framework of current HomePlug networks but can become possible with the HomePlug AV generation.

The main difficulty for these two applications is to control synchronizations to replay images in time. The same two techniques used for telephone speech can be implemented to carry out this synchronization priority management at the IP level or HomePlug frame level. The second solution makes it possible to assign a priority on the random access of the MAC layer and grant shorter timers to stations with priority. In other words, the priority stations take precedence over the other ones as long as they have frames to transmit. The only condition to be observed is that the total bit rates of the priority stations remain lower than the value of the useful throughput available.

In HomePlug 1.0 PLC networks, broadcasting good quality videoconferencing cannot be envisaged easily. With HomePlug AV extensions to 200 Mbit/s (nominal transfer rate), if the number of clients is reduced, it then becomes possible to transmit over one or two good quality videoconferencing channels although the probability of desynchronization quickly increases with the traffic.

Multimedia

Multimedia applications generally use at least one speech or video stream superimposed onto other data streams. These applications do not pose more problems for PLC networks than telephone voice or video. The only additional constraint that they bring about comes from the synchronization of the simultaneous applications that achieve the multimedia process.

A compromise must be achieved between the complexity and the transit time in the networks to convey multimedia applications. To find again the quality of the original signal for digital documents, we consider that the compression must be lim-

ited to a factor 3. This is the case of imaging applications, in which the quality is essential, such as X-ray radiographies, for example. Factors varying from 10 to 50 for fixed images and from 50 to 200 for video are obtained. The compression average is 20 for fixed images and 100 for video.

These compressions distort the image very slightly but use the recovery capacities of the human eye. This is because the eye is much more sensitive to luminance, i.e., image brightness, than to chrominance or color. This characteristic is found again in the coding of the high definition television, where the luminance resolution is based on an image definition of 720 by 480 points, whereas a definition of 360 by 240 points is used by the chrominance signal. The luminance requires more coding bits per point than the chrominance.

We have seen that the PLC networks can support the necessary bit rates to transmit the streams of multimedia applications. For this purpose, the number of clients with access to an electrical network just needs to be limited (see Chapter 3).

Therefore, the problem resides less in the network capacity than in the management of time constraints. The two constraints (real time and synchronization) are very difficult to achieve with asynchronous networks such as PLC networks, in which there is no time management and where data is not transported in a determinist way (see Chapter 3).

In this respect, HomePlug AV is essential for transporting multimedia applications, since it is the only one that can classify packets according to priorities in order to obtain the quality of service necessary for the applications transported by each stream.

Quality of Service

As we have seen in Chapter 3, no quality of service is proposed by HomePlug 1.0 and Turbo in their technology, since the data transfer times are not determinist. The quality of service must be implemented by the application layers above the MAC layer to compensate for this nondeterminism.

An implementation of the quality of service is proposed by HomePlug AV with a guarantee for the various services requiring a bit rate and a stable data transfer time. This quality of service is provided by the allocation of TDMA timeslots for each type of data service.

Table 6.1 gives examples of subscriber premises PLC networks according to utilization scenarios (lone couple, couple with three young children, and couple with a young child and two teenagers).

PLC Local Networks

The use of PLCs to build a local area computer network is the most visible and widespread among the general public and professionals. Families are keen to equip themselves with several personal computers to share a number of applications and access to the Internet, whereas professional environments exchange occupational and Internet applications.

Table 6.1 Subscriber Premises PLC Network Utilization Scenarios

APPLICATION	*NECESSARY BIT RATE*	*UTILIZATION SCENARIO*					
		Lone couple		Couple with three young children		Couple with a young child and two teenagers	
		Qty	Bit rate	Qty	Bit rate	Qty	Bit rate
Home cinema HDTV	22 to 28 Mbit/s	1	22 to 28	1	22 to 28	1	22 to 28
IPTV	3 to 7 Mbit/s	1	3 to 7	3	9 to 21	2	6 to 14
Home theater digital audio system	5.4 Mbit/s	1	5.4	1	5.4	1	5.4
Digital audio CD	2 × 0.8 Mbit/s					3	4.8
Telephony over IP	(0;064 + 0.016) = 80 Kbit/s (codec G.711)	2	0.16	2	0.16	3	0.24
IP data	2 Mbit/s	2	4	2	4	5	10
TOTAL		6	34.5 to 44.4	9	40.6 to 58.4	15	48.4 to 62.2

Internet Connection Sharing

One of the most usual PLC applications relates to the sharing of the Internet connection between several terminals or computers of the same network.

PLC technology makes it easy to network the various house or office computers and to connect them to the Internet connection modem through the electrical network. The architecture of such a network then appears as illustrated in Figure 6.4. The PC connected to this network by PLC devices retrieves the signal via the electrical network. One of the major advantages of PLCs is that any outlet in the home can retrieve the Internet signal.

As illustrated in the diagram, the bit rate is shared between the various network users where the Internet connection bandwidth is divided by the number of users.

File and Printer Sharing

A PLC local area network makes it possible to complement all the applications found in the wired or wireless subscriber premises or in professional computer networks.

File sharing and printer sharing (see Figure 6.5) are two of the most frequently used applications:

- *File sharing*. A server connected to the electrical network by using a PLC device hosts the files to be shared between the network users. These users connect to this server via the electrical network and correctly configured PLC devices.
- *Printer sharing*. Likewise, the printer can be placed at a favorable location of the house or business premises and connected to the PLC network using its

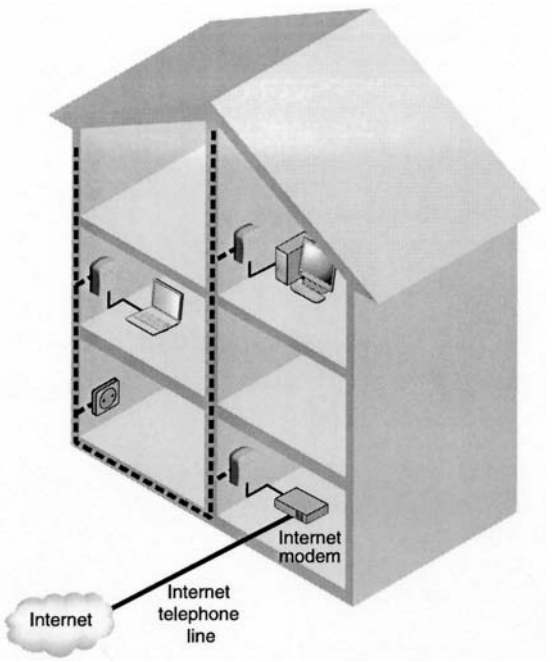

Figure 6.4 Internet connection sharing

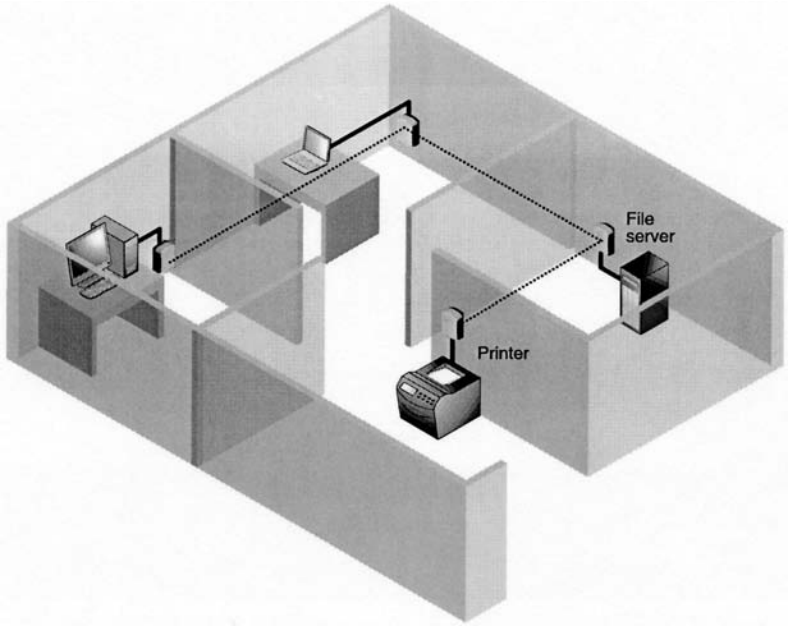

Figure 6.5 File and printer sharing in a PLC local area network

Ethernet interface (RJ-45 connector). From then on, the other users can use it as a network printer with its IP address.

Audio Broadcasting

A PLC local area network enables data broadcasting over the electrical network including audio data (see Figure 6.6) originating from various sources, in particular the following ones:

- *Audio file servers*. The files are in MP3 or WAV format and are sent over the electrical network to be retrieved by PLC devices connected to the installation hi-fi devices.
- *Hi-fi system*. The audio signal from one hi-fi system to another or to audio speaker systems can be shared. In the second case, the electrical network replaces the audio/stereo cables used to connect between the hi-fi system and the audio speakers.

Recreational Applications

Recreational applications (video games) increasingly use the computer networks to connect the various players between them. Games terminals fitted with a network interface can use the electrical network for connection purposes exactly like in the case when file sharing over a PLC local area network.

Video Surveillance

The widespread use of IP cameras fitted with Ethernet network interfaces (RJ-45 connector) means they can be connected to a PLC local area network via electrical outlets. This provides a high flexibility in the placement of cameras that must in any way be powered by a nearby outlet. Figure 6.7 illustrates this application.

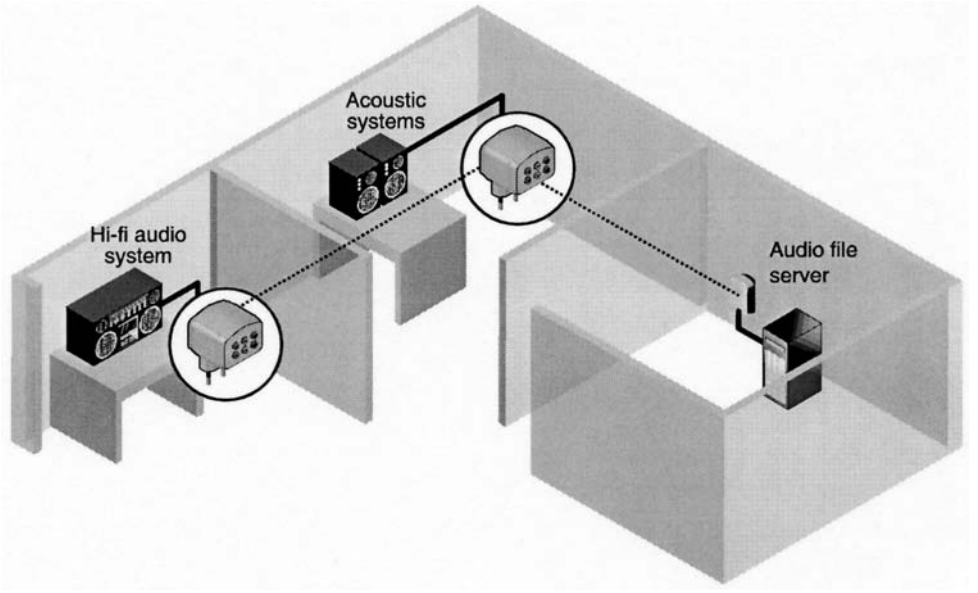

Figure 6.6 Audio broadcasting in a PLC network

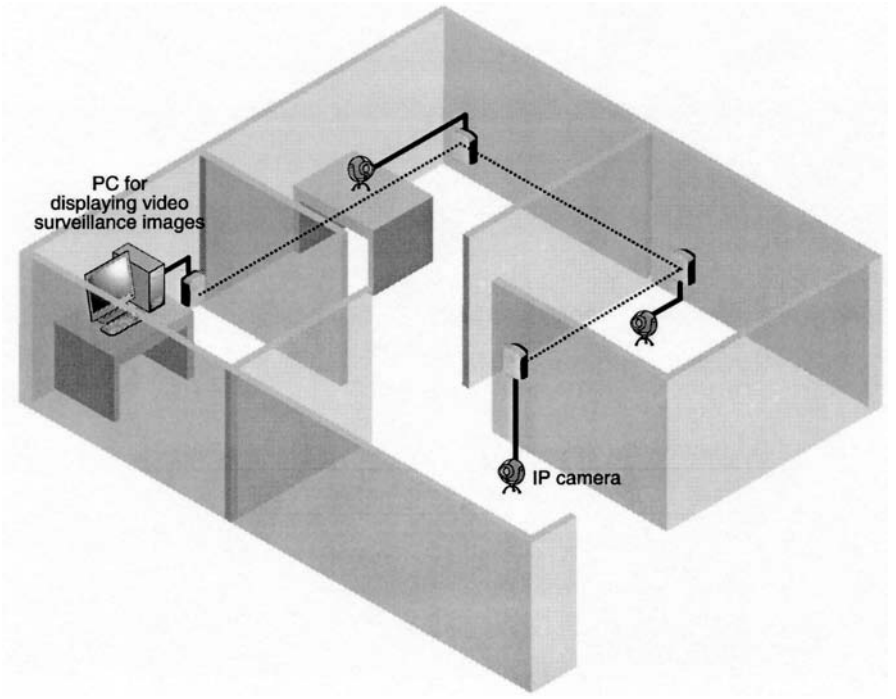

Figure 6.7 Video surveillance on a PLC local area network

Backbone of a Wi-Fi Network

As we'll see in Chapter 13, dedicated to hybrid networks, each computer network technology has advantages and disadvantages.

A radio computer network that provides both mobility and flexibility to the users within the building where the network is installed can be built with Wi-Fi. However, the hardware constraints of this technology make it necessary for it to be based on a wired Ethernet backbone for full coverage of the building. This role of Ethernet backbone can be attributed to a PLC local area network by connecting the Wi-Fi access points to the electrical network.

Figure 6.8 illustrates the architecture of this network type in which each Wi-Fi access point forming a radio cell is connected to the network by a PLC device.

InternetBox and PLC

Many Internet access providers in Europe, such as Orange, Free, Neuf-Cegetel, Alice, Club-Internet, Vodafone, Belgacom; in the USA, such as Comcast; or in Asia like NTT in Japan now offer solutions for accessing Internet "multiplay" services through an InternetBox, particularly the following:

- *Data*. The InternetBox is above all a modem to access the Internet with, enabling users to access data services such as the Web, messaging, FTP, IRC, P2P, and so forth.

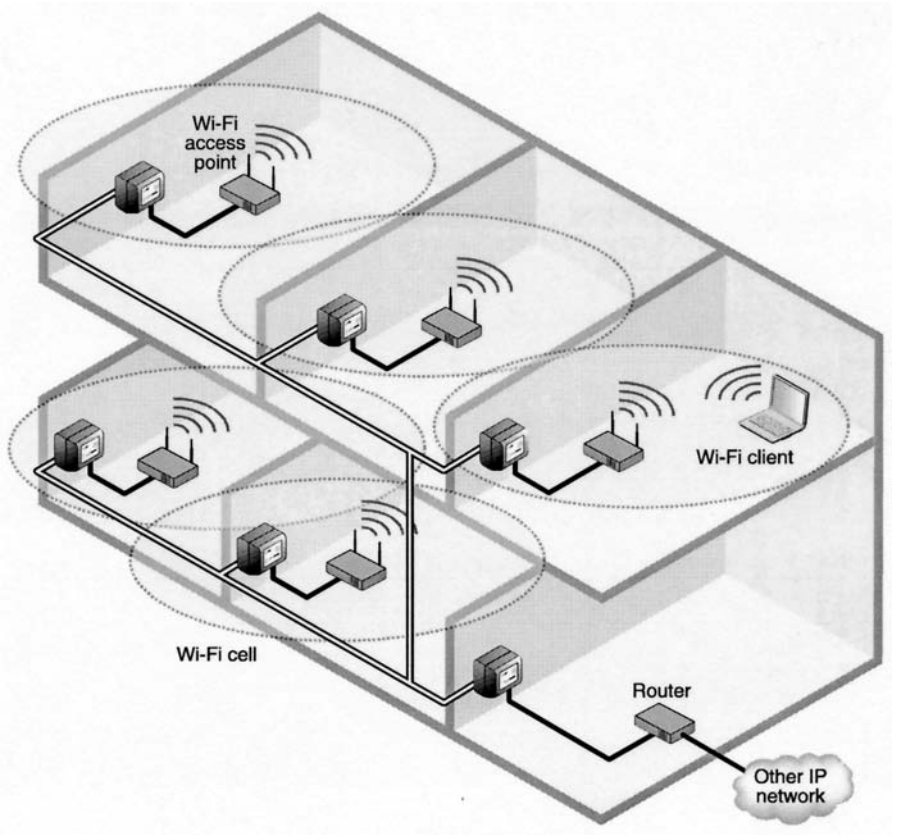

Figure 6.8 PLC local area network used as the backbone of a Wi-Fi network

- *Voice*. Telephony over IP services. The InternetBox behaves like a telephone receiver to which the analog telephones used on the switched telecommunications network (STN) are connected.
- *Video*. IPTV for the broadcasting of TV channels over IP networks and video on demand (VoD).
- *IP services*. Domestic mobile telephony, home automation (like electrical power management and family server), and so forth. These services will turn the InternetBox into a true smart gateway in the near future.

Each of these services must be routed to the end user (television set, telephone, computer, IP household appliances, and so forth) via an Ethernet network. For this purpose, the PLC local area network is an excellent solution as it uses a network available in any building.

As illustrated by Figure 6.9, these services require an Ethernet link between the InternetBox and the video decoder or the telephones; this link can be provided by PLC devices.

Internet access providers already provide the following devices integrating PLC products or completed by them:

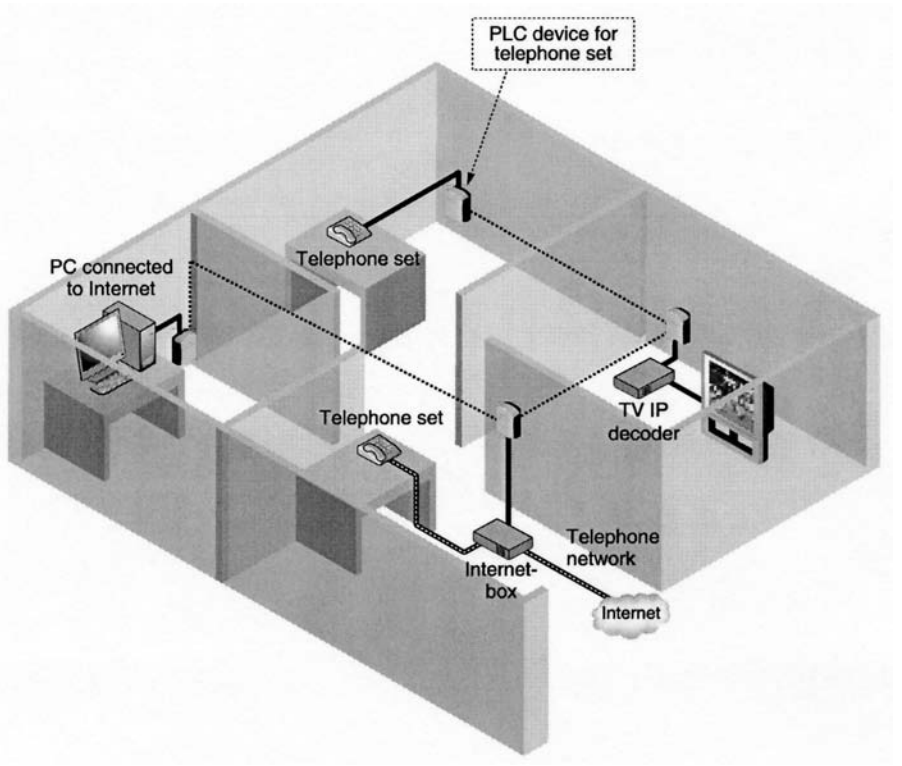

Figure 6.9 InternetBox and PLC

- set-top boxes;
- TV decoders;
- electrical over-plugs;
- flat screens.

New Applications for PLC

The maturity of PLC technologies convinced some manufacturers to use PLC as the transmission medium for applications that until then were not networked at all, or available only over proprietary and expensive networks.

The fact that an increasing number of industrial devices have a network interface makes it possible to build new types of networks allowing connection, in particular in boats, public spaces, and automobiles.

PLC in Industry

In the industrial world, the application constraints are more severe than in general public or professional local area networks. Until now, these constraints have slowed down PLC development, but the maturity of HomePlug and the initial feedback from the deployments of PLC networks led to the ration consider of PLCs as a viable solution for connections between machines.

The industrial applications that currently use PLC networks are the following:

- sensor networks;
- connection of programmable controllers;
- PC located in confined spaces where wiring is difficult (on top of a crane, in spaces with metal piping making it impossible to use Wi-Fi, and so forth).

PLC in Public Spaces

Like in the industrial world, more and more public spaces now have communicating devices or devices fitted with Ethernet interfaces ready to be connected to a local area network.

Many applications already use PLCs to connect these devices, particularly the following:

- content distribution toward interactive terminals;
- information feedback from beverage dispensers;
- authentication traffic for time clocks.

PLC over Coaxial Cable

As we'll see in Chapter 7, dedicated to devices, the PLC can use not only 110-220V 50-60 Hz electrical wiring but also other wiring types to convey the signal in the 1 to 30 MHz band. One of the wirings that is the most used by PLC devices is the coaxial cable conventionally used by cable operators to broadcast the TV signal originating from cable television channels.

This cable has very interesting propagation and interference immunity (since the cable is protected and even shielded) characteristics used for transporting the PLC signal. Therefore, the coaxial cable can advantageously complete an electrical network when building a PLC network in order to compensate for certain types of topology problems related to the use of the electrical network only (network too old, electrical network too complex with respect to the application requirements, and so forth).

PLC Without Electrical Current

The propagation of the PLC signal over the electrical wiring does not require the 110 to 220V/50 to 60 Hz power signal. A PLC network can be imagined without electrical operation in the building as long as the PLC devices can be powered in one way or another from a battery. From then on, they can use the electrical network to communicate between themselves but without drawing off their power from it. This original PLC application can prove useful in the case where the mains are cut off and in the case where certain types of battery operated computing equipment still want to communicate during the cut-off time.

PLC in Motor Vehicles

Automobiles increasingly need to transport internal data between the various controls and the instrument panel. These information exchanges require wiring of up to 3 km in length and 50 kg in weight.

In Europe, the Valeo component manufacturer and the company manufacturing PLC products worked together to implement a solution using PLC to communicate the information from the vehicle sensors to the instrument panel.

This type of PLC network can also be used to broadcast external camera or onboard DVD drive videos.

Economic Perspectives

As we have seen in this chapter, most applications transported by the electrical networks face multiple constraints inherent in PLC (i.e., bit rate, topology, and also number of users in the network).

The number of these applications goes on increasing, but most of them are already available in the conventional networks, like voice or video.

The number of PLC terminals also constantly increases, and nowadays PLC products can be found with most resellers of data processing and network equipment.

Therefore, PLC must be considered not only as a network technology but also as a simple means to connect devices together by allowing information sharing. The emergence of PLC in the hi-fi world is a striking example of this. A central server connected to the Internet can deliver any type of flow (video or audio) to any device (LCD screen or mini-system) located in the house by means of PLC links.

Therefore, the economic perspectives for PLC networks are high, in particular for the following reasons:

- Emergence of HomePlug AV products in the course of 2009.
- Commitment of Internet access providers to widen the distribution of InternetBox services to housing. In the long run, this strategy will generalize the use of PLCs among the general public.
- Growing understanding by the general public of a technology that is now mature and particularly simple to use (no new wiring, use of existing outlets, simplified configuration, security, and so forth).
- Understanding by professionals that PLC networks complete cables and Wi-Fi, in particular with the development of PLC products dedicated to the requirements related to the administration and management of professional networks.

Figure 6.10 illustrates the expected growth of PLC networks by 2010. Its easy deployment combined with lower costs for the devices and the development of products combining several technologies (gateway, router, modem, firewall, server, and so forth) undoubtedly ensure that this technology has a great future ahead.

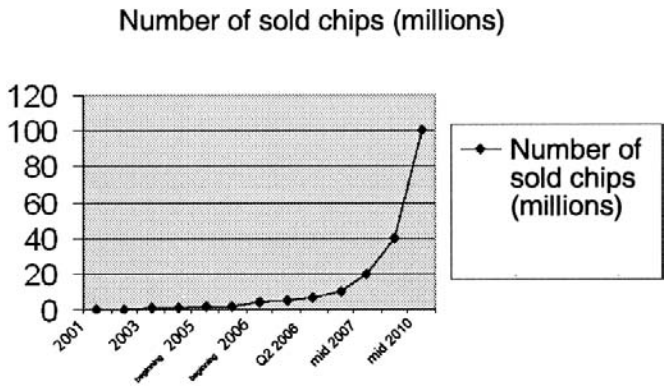

Figure 6.10 Number of HomePlug chips sold worldwide

CHAPTER 7

Equipment

Since the emergence of the HomePlug 1.0 specification in 2003, the PLC network equipment market has continued to grow. Originally focused on small networks with a low bit rate and few computers, it then turned to private individuals very keen on a technology enabling Internet connection sharing while eliminating wiring constraints and remaining relatively easy to use with the support of Internet access providers.

This chapter will cover all the PLC products currently available on the market for connecting terminals to the local area network, to build or to optimize the PLC network (filters, repeaters, injectors, and so forth).

PLC Technologies

Since the appearance of the first high speed PLC devices, several technologies have been developed, but no international standard has appeared for the time being.

In the technologies offered to the public, several approaches have been implemented, in particular the following ones:

- choice of the network mode;
- modulation techniques;
- number of sub-bands;
- MAC layer implementation.

With over 90% of the PLC equipment market, HomePlug technology is so widespread that it's becoming the standard product.

The various PLC technologies are summarized in Table 7.1 depending on the network mode chosen.

The various network modes (master-slave, peer-to-peer, and centralized) are used by the PLC technologies according to the constraints of each application. Ascom and Itran were among the first to develop Ethernet interface-based PLC equipment. They first gave preference to the master-slave mode for its centralized administration capacities.

Table 7.1 PLC Technologies According to the Network Mode

TECHNOLOGY		*MODE*
Ascom APA 450 (4.5 Mbit/s)		Master-slave
Itran (Main.net) PLTNet & ITM1 (2 Mbit/s)		Master-slave
HomePlug	1.0	Peer-to-peer
	1.0 Turbo	Peer-to-peer
	AV	Centralized
DS2	DSS4200 (45 Mbit/s)	Peer-to-peer
	200 Mbit/s	Master-slave
Spidcom	45 Mbit/s	Peer-to-peer
	SPC200 (200 Mbit/s)	Master-slave

Master-Slave Mode

Figure 7.1 illustrates the architecture of an LV (low voltage) PLC network for electrical distribution in the master-slave mode. We find the master device at the MV/LV (medium voltage to low voltage) transformer level. This device checks the good working order of the PLC network and more particularly the existing network links with the slave devices located between the electrical meters of the houses.

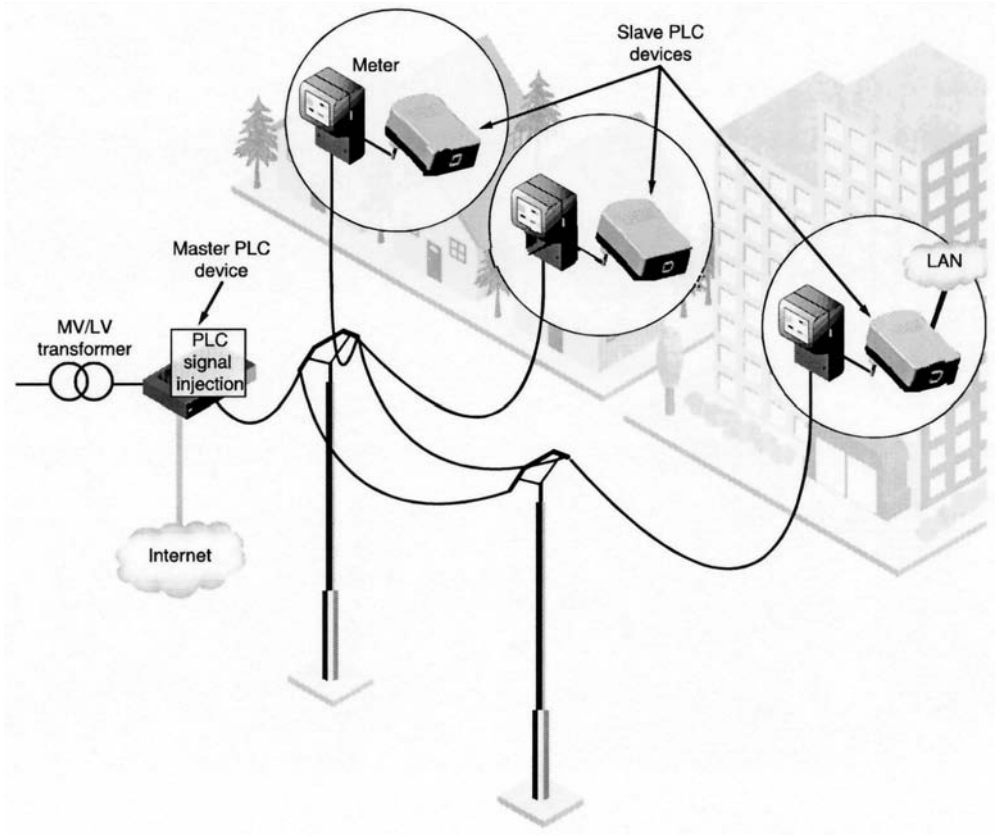

Figure 7.1 Simplified architecture of the master-slave mode

Figure 7.2 illustrates another architecture in the master-slave mode in a domestic electrical network. Here we find conventional private electrical network devices of which we had an overview in Chapter 2.

The electrical switchboard controls electrical wirings, power outlets, bulbs, and electrical devices. The cables connected to the electrical switchboard are generally known as "bus-bar electrical connections," since they start from a central point (electrical switchboard) and run right across the building according to the power supply requirements.

In this topology, the master PLC device is ideally located at this central point (electrical switchboard). The slave devices consist of the outlets scattered along the electrical network.

The master equipment acts as a gateway between the fixed telephone network (connected to a modem for access to the Internet, for example) and the PLC local area network, which uses the electrical network. This device is also in charge of managing the network and the various slave devices.

Table 7.2 summarizes the main advantages and disadvantages of the number of bus-bar electrical connections.

There are many PLC device manufacturers who have chosen the master-slave mode, notably the following:

- *Main.net*. Develops products for public LV electrical networks that give preference to this mode in order to match the topology of the electrical networks.

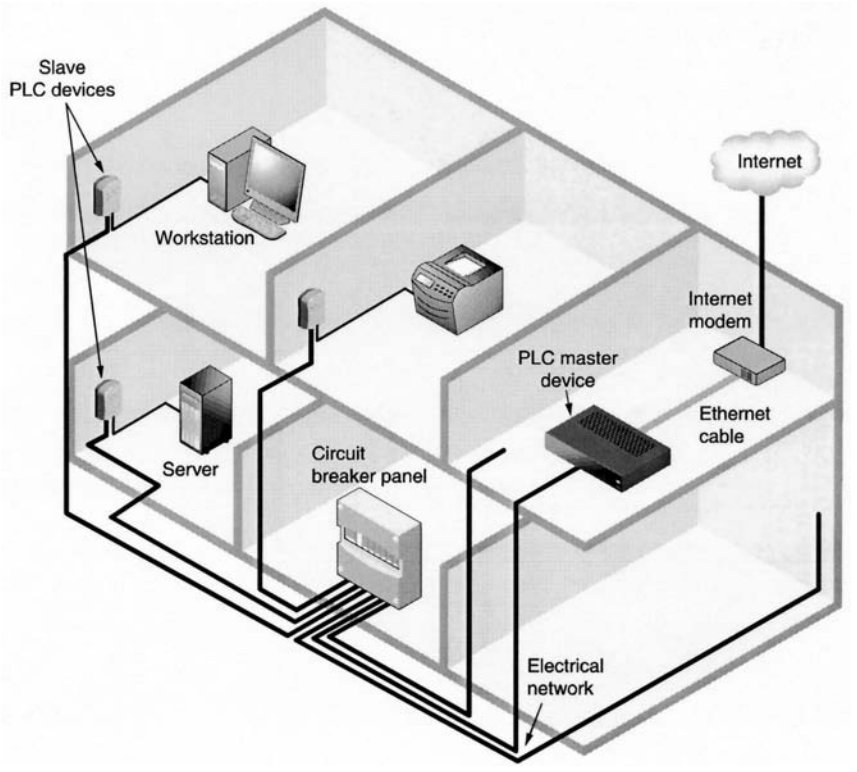

Figure 7.2 Equipment position in a domestic LV PLC network in the master-slave mode

Table 7.2 Advantages and Disadvantages of the Number of Bus-Bar Electrical Connections

NUMBER OF BUS-BAR CONNECTIONS	*ADVANTAGES*	*DISADVANTAGES*
Single bus-bar connection	– Easier design – Potential repetition with master devices – Easier supervision	– Divided bandwidth – Possible multipaths for circulating frames – Loop possibility
Several bus-bar connections	– Broader network coverage – Separation of useful networks	– More complicated supervision

Conventionally, this is a star topology. The MV/LV transformer used as the injection point of the PLC signal is located in the middle of the star and the PLC devices of the end users are placed at the ends of the various bus-bar electrical connections from the transformer.

- *Ascom.* Develops products for public and domestic LV electrical networks using this mode since 1998. This generation of products provided a 250 Kbit/s speed. One of the devices was used as the master, whereas the other ones were slaves. The configuration was carried out in Telnet mode or using configuration files and a TFTP client-server system.
- *DS2 and Spidcom.* After having used the peer-to-peer mode to deploy it more easily, these two manufacturers are now developing products in the master-slave mode to benefit from a centralized administration and better QoS management for allocating TDMA frames for real-time applications like video.

Case of Ascom APA Devices

Ascom APA devices with a 4.5 Mbit/s speed represent one of the very first generations of high speed PLC equipment. The master device was accessible by means of a Telnet interface for the device configuration and then could be supervised from a v2/v3 SNMP administration console. The master could manage 63 slaves maximum.

Figures 7.3 to 7.6 illustrate the Ascom APM 45 master and slave devices.

Some PLC devices are used for remote telephone interfaces over the PLC network. The Phonex company, for example, develops devices with RJ-11 interfaces to carry voice analog communications over the electrical network.

Peer-to-Peer Mode

In the master-slave mode, a master device is at a higher hierarchical level (it manages and controls the network) and the slave devices are at a lower hierarchical level (their function is limited to communications with the master device). In peer-to-peer mode, all the devices have the same hierarchical level and exchange data with all the other PLC devices of the network. Therefore, the network consists of *N* to *N* links.

Figure 7.3 Master device managing the ASCOM Powerline APM-45o PLC network

Figure 7.4 ASCOM Powerline APA-45i slave device used for the connection of client terminals to the PLC local area network

Figure 7.5 Slave device interfaces

As illustrated in Figure 7.7, the peer-to-peer mode is ideal for local area networks since the LAN architecture must enable any terminal (typically PC) to exchange data with any other LAN terminal. HomePlug 1.0 and Turbo use this mode.

Centralized Mode

As we have seen in Chapter 3, HomePlug AV uses the centralized mode, which is a combination of the master-slave and peer-to-peer modes.

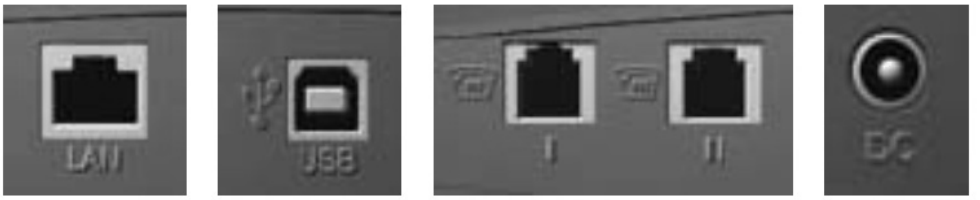

Figure 7.6 Details on the RJ-45, USB, and RJ-11 Ethernet LAN interfaces of the slave device

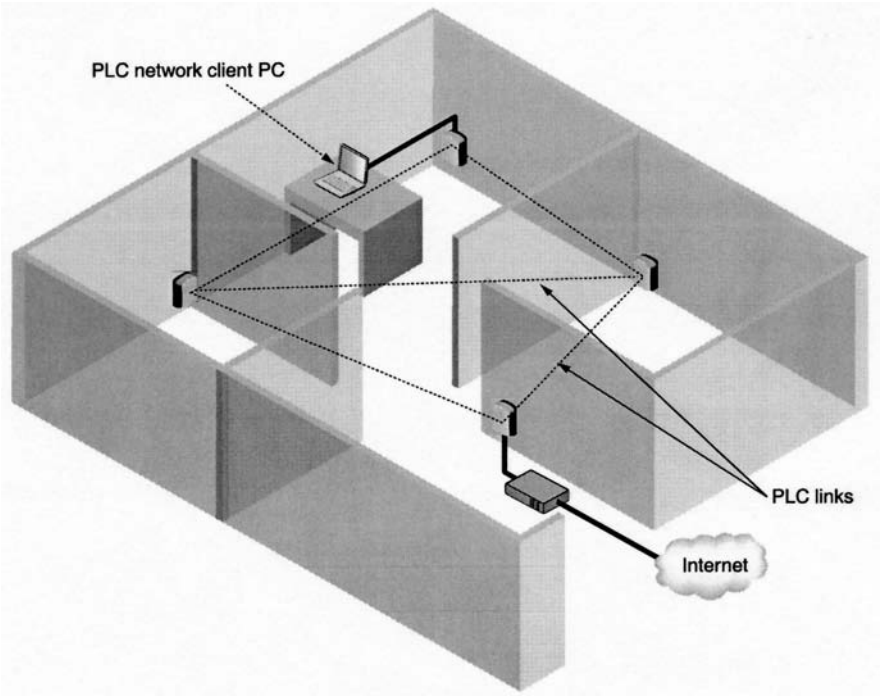

Figure 7.7 Architecture of a PLC network in peer-to-peer mode

In HomePlug AV PLC networks, one of the devices acts as the central device and manages the communications between the PLC stations of the network. The exchanges between PLC stations directly take place without going through the central device. However, the stations must identify with the central device and comply with the time allocations given by the central device.

PLC Modems

As PLC technology intrinsically uses the electrical network, the PLC devices, irrespective of their nature, connect to the outlets or directly inject the signal into the electrical wirings. The signal injection, which allows a PLC device to connect directly to the electrical wiring, is described later in this chapter.

Although the PLC technology does not use the modulation-demodulation process implemented in the modems, we talk about a PLC modem to designate the device to which the terminals that want to take part in the PLC network are connected.

Unlike Wi-Fi interfaces, which are integrated into the terminals in the form of boards, the PLC interfaces are not integrated into the terminals. Therefore, the terminal, which is generally a computer, connects to the device that has two interfaces: one for the connection to the electrical network, and the other one (RJ-45 or USB) for the connection to the terminal.

The PLC modem, which is the most widespread device in the PLC networks, is also the easiest to use, since it appears as a standard electrical appliance fitted with a male receptacle to be connected into an outlet and a USB or Ethernet interface to be connected to the terminal.

When viewed from the outside, a PLC modem therefore has the two following interfaces:

- male receptacle;
- RJ-45 Ethernet or USB network interface.

The modem generally has three indicators (LED) that indicate the presence of the 110 to 220V/50 to 60 Hz, PLC signal on the electrical interface and that of the Ethernet network on the RJ-45 interface to the user (see Figure 7.8, left).

Some devices have up to five indicator lights so that the user can check that the device is in good working order.

Dissipation in PLC Modems

The first HomePlug 1.0 PLC devices in plastic packages had heat dissipation problems due to the permanent 110-200V/50-60 Hz power supply. This resulted in failures of the electronic components that did not withstand heat for long periods in the packages.

The PLC devices have been improved with the emergence of more robust components, cooling fins, and vent holes (see Figure 7.8, right) so that they can operate correctly even in situations in which the devices were stacked or placed in poorly ventilated environ-

Figure 7.8 Outside and inside of a HomePlug Corinex PowerNet PLC modem

ments and at temperatures that can be as high as 70°C and are made of plastic for consumer equipment and of metal for professional equipment.

Inside the package, the entire hardware architecture is structured around the main component (HomePlug PLC chip, see Figure 7.8, middle). The Intellon manufacturer is the main supplier of HomePlug chips.

Table 7.3 summarizes the various versions of chips that appeared as the HomePlug technology has progressed.

Around this PLC chip that implements all the functionalities of the PLC networks introduced in Chapter 3, a number of components and electronic circuits are used to optimize the operation of the PLC modem:

- Coupling to the electrical network (i.e., PLC modem connection to the electrical network).
- PLC signal gain control for optimized data emission/reception, including under difficult conditions, due to noises on the electrical network in particular.
- Storage of information on the PLC network state. This function is provided by an EPROM (persistent memory when restarting the modem) and a SRAM (volatile memory erased when restarting the modem), which keep information on the state of the PLC links, network encryption keys, or access authorization.

Figure 7.9 illustrates the hardware architecture of a HomePlug 1.0 PLC modem.

The manufacturers have developed two types of PLC modems: "desktop" modems, which appear as packages to be placed on a table or on a pedestal, with a cord to connect to outlets; and "wallmount" modems, which appear as integrated packages directly connected into outlets. Most PLC modems are wallmount modems since they are easy to use.

Figure 7.10 illustrates examples of wallmount (left) and desktop (right) modems.

PLC USB Modems

PLC USB modems offer a USB interface so they can be connected to the USB ports of computers or network terminals. The USB port acts as a virtual network interface card for connection to the PLC network.

The interest of these modems resides in the fact that all computers do not have a network interface card whereas they are all fitted with USB ports. However, they are not as simple to configure as an Ethernet PLC modem.

Table 7.3 Models of Intellon Chips

HomePlug	*CHIP*
1.0 (also called 1.0.1)	INT5130, INT51MX
Turbo (also called 1.1)	INT5500
AV	INT6000, INT6300

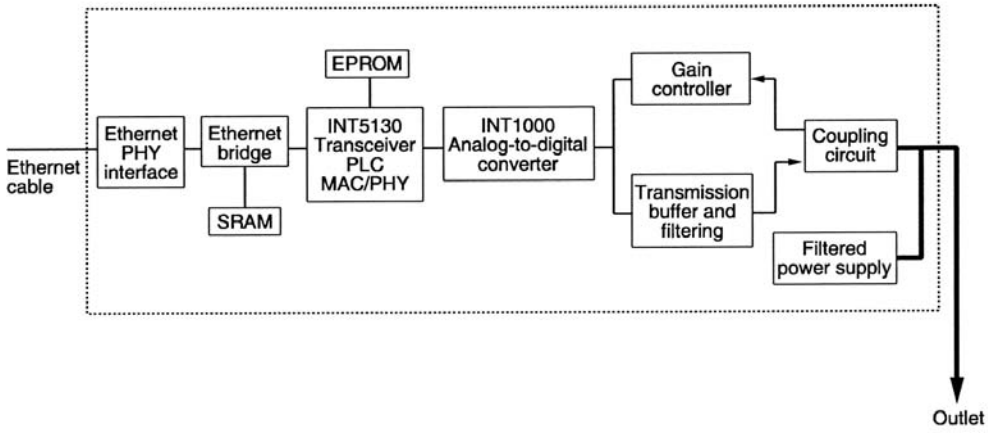

Figure 7.9 Hardware architecture of a PLC modem

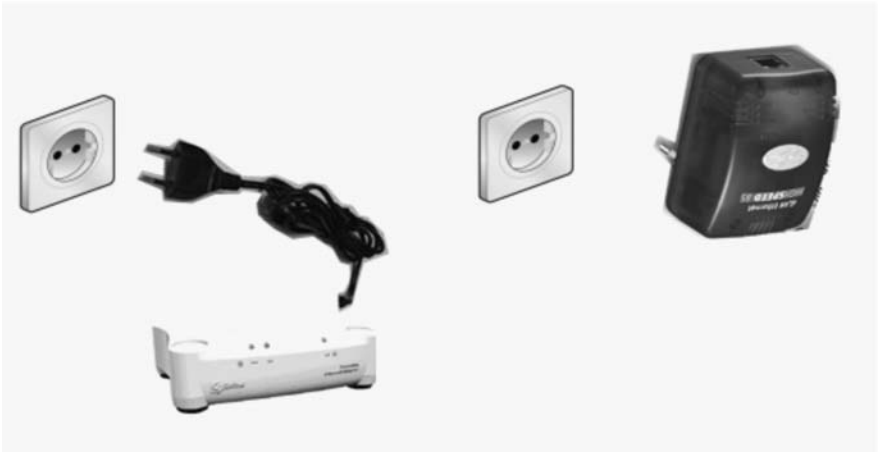

Figure 7.10 Wallmount and desktop PLC modems

Figure 7.11 illustrates a F@st Plug type Sagem USB PLC modem.

PLC Ethernet Modems

The generalization of network interface cards in computers, network terminals, and electronic devices, even in household appliances, simplifies the building of networks by using the Ethernet board's RJ-45 connectors.

This type of modem has become the most widely used PLC device. As well as being simple to use and configure, its price continues to fall.

Figure 7.12 illustrates a Devolo Ethernet PLC modem of the dLAN Ethernet HighSpeed 85 type.

The Ethernet network interface card of PLC modems was the first of the 10 baseT type (10 Mbit/s) for HomePlug 1.0 modems providing a maximum useful throughput at the MAC layer level of 8.2 Mbit/s, then of the 100baseT type (100 Mbit/s) for HomePlug Turbo and AV modems.

Figure 7.11 F@st Plug type Sagem USB PLC modem

Figure 7.12 Devolo Ethernet PLC modem of the dLAN Ethernet HighSpeed 85 type

The increased performance of HomePlug PLC devices will probably lead the manufacturers to use 1,000baseT (1,000 Mbit/s) boards so that the throughput is not limited over the Ethernet interface. It would not be surprising to come across optical fiber PLC devices.

The Devolo company offers devices with the two USB and Ethernet interfaces.

Figure 7.13 illustrates a Devolo PLC modem of the dLAN duo type with USB and Ethernet interfaces.

Figure 7.14 illustrates Devolo PLC modems complying with the HomePlug AV standard with, on the left, a consumer wallmount-style model, in the middle, a professional desktop model and, on the right, a professional wallmount model with Ethernet and USB interfaces.

PLC Cable TV Modems

Some manufacturers of PLC modems offer PLC devices used for the connection to a cable television network. These devices are highly immune to electromagnetic disturbances.

The two following frequency bands are used by cable TV:

- data in the 1 to 24 MHz band;
- TV signal in the 47 to 862 MHz band.

Figure 7.13 Devolo PLC modem of the dLAN duo type with USB and Ethernet interfaces

Figure 7.14 Devolo Homeplug AV PLC devices

The networks of cable operators are much less widespread than the electrical network and generally have few TV sockets. However, such networks can end up complementing the electrical network due to their relatively constant speed, which in any case is more stable than that of the electrical network.

Since a cable TV network is a shared network, its speed is divided by the number of users on the medium.

The PLC cable TV devices use several types of connectors, in particular F-type connectors for connection to cable TV. Over a cabled network, the propagation distance generally is 500 to 700m while keeping a high useful throughput.

Figure 7.15 illustrates, from the left to the right, a Corinex CableLAN cable TV PLC modem, coaxial cables, a F-type connector, and a Channel Vision splitter.

PLC cable TV modems have evolved at the same time as the HomePlug technologies and their bit rate. These modems can be used for the two following applications:

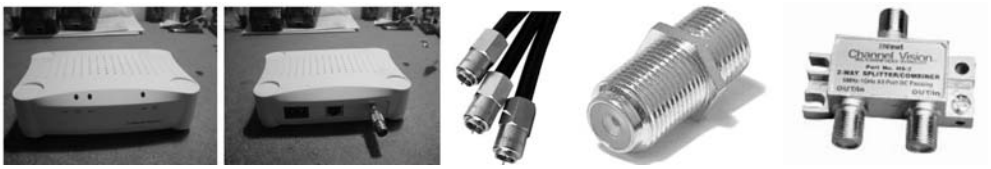

Figure 7.15 Corinex CableLAN cable TV PLC modems, TV cables, F-type connector, and splitter

- data circulation over the cable television network to make it the backbone of the PLC network;
- use of the coaxial interface with an adapter called "injector" (see later in this chapter) used to emit the PLC signal directly over the electrical wiring without using outlets.

Although these PLC modems use a medium that is not the electrical wiring, they are compatible with HomePlug via HomeNetworking technologies such as HomePNA (Home Phoneline Network Alliance) or UPA (Universal Powerline Association).

Table 7.4 gives the bit rates of the main PLC cable TV modems according to the technology used.

The HomePNA standard also enables the use domestic telephone cables to convey data. The Corinex company markets the CableLAN Combo Adapter product in particular, which uses the HomePNA 3.0 standard and has two interfaces: a coaxial interface (F-type connector) and a telephone interface (RJ-11 connector).

PLC Modems Integrated with Electrical Outlets

Some manufacturers offer PLC modems directly integrated with electrical outlets.

The Lea and Legrand companies have developed a PLC outlet, called "SmartPlug," which integrates a HomePlug PLC modem into the outlet unit and Ethernet RJ-45 connectors. The SmartPlug schematic diagram is illustrated in Figure 7.16.

PLC/Wi-Fi Modems

As we'll see in Chapter 13, dedicated to hybrid networks, the PLC and Wi-Fi technologies fully complement each other and enable users to build a complete network with optimum radio coverage. The PLC network acts as the backbone of the Wi-Fi network in order to provide a better radio coverage to this network.

The latest evolutions of the HomePlug technology make it possible to compare the performance of the two technologies. HomePlug Turbo provides a maximum useful throughput at the physical level of 85 Mbit/s, and the IEEE 802.11g standard of 55 Mbit/s. The PLC/Wi-Fi devices make it possible to benefit both from easy PLC use and Wi-Fi mobility.

Some of these devices integrate PLC and Wi-Fi components whereas other devices provide PCMCIA slots in a PLC modem enabling the user to use the best Wi-Fi board for his or her radio network.

Table 7.4 Bit Rates of the Main PLC Cable TV Modems

PLC CABLE TV MODEM	*TECHNOLOGY*	*BIT RATE (Mbit/s)*
Corinex CableLAN	HomePNA 1.0	10
Corinex CableLAN AV	HomePNA 3.0	128
Corinex CableLAN 200	Pre-UPA	200

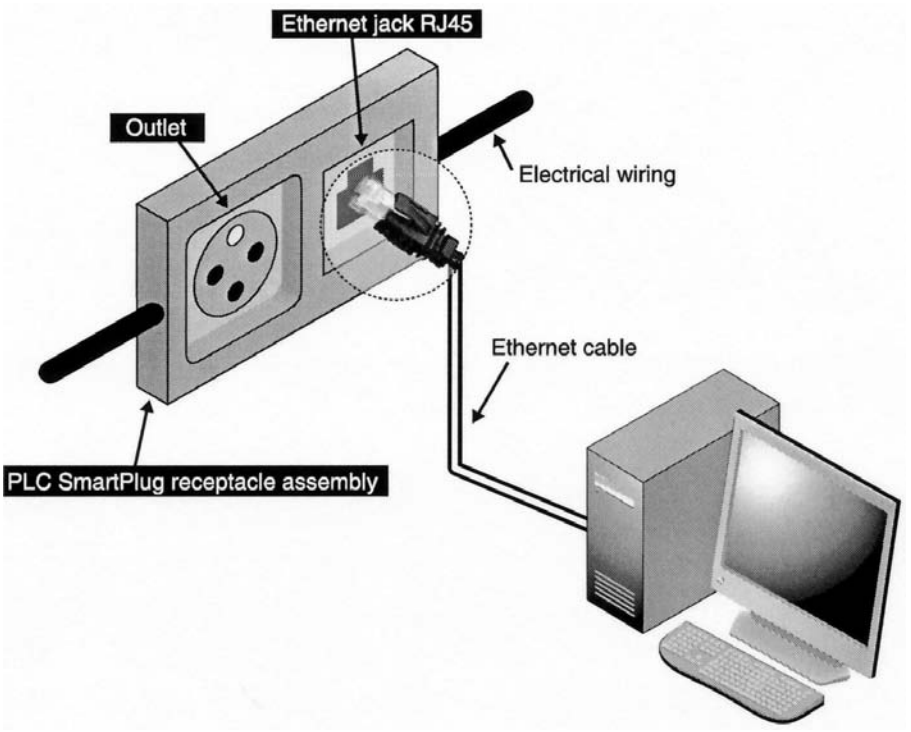

Figure 7.16 LEA-Legrand SmartPlug PLC outlet schematic diagram

Figure 7.17 illustrates Thesys (on the left) and Devolo MicroLink dLAN Wireless (on the right) PLC/Wi-Fi modems.

Some manufacturers are currently working on the optimization of the MAC layer between PLC and Wi-Fi in order to increase the reliability of these hybrid networks and their performance at the MAC layer level. These projects should result in products marketed in 2009.

One of the optimal PLC applications as a supplement to Wi-Fi consists of using the lighting system of a building to build a PLC backbone and placing the PLC/Wi-Fi devices close to the bulbs.

The Taiwanese company Lite-on offers the ORB product appearing as a Wi-Fi PLC bulb that, in addition to its function as a lightbulb, is used for the efficient diffusion of the Wi-Fi radio signal in the room. This bulb is PLC connected both to the lighting system and to the other PLC or PLC/Wi-Fi devices of the lighting system and of the supply power system.

Multifunction PLC Modems

Some PLC products include various network functions meeting the requirements of network engineers as well as users, in particular the following ones:

- Ethernet PLC/hub modem used to connect several PCs to the same PLC Ethernet modem.

Figure 7.17 Thesys and Devolo PLC/Wi-Fi modems

- ADSL/router PLC modem used to transmit the signal originating from the Internet connection over the electrical network. Some devices even add a Wi-Fi board.

Figure 7.18 illustrates Hub Netgear (on the left) and Thesys NetPlug (on the right) PLC modems.

Figure 7.19 illustrates a Devolo dLAN ADSL modem router PLC device.

PLC Audio and Telephone Modems

Since PLC allows data to circulate over the electrical network, some manufacturers have been developing audio and telephone PLC products for a long time.

An audio PLC modem connects to the electrical network on the one side and to a hi-fi device, such as an audio speaker, an audio system, an audio file server, and so forth, on the other.

Figure 7.20 illustrates a Devolo MicroLink dLAN Audio PLC modem with Cinch (two for Out channels and two for In channels), SPDIF (one for In channel and one for Out channel), and Audio Jack (one for In channel and one for Out chan-

Figure 7.18 Hub NetGear and Thesys NetPlug PLC modems

Figure 7.19 Devolo ADSL/router PLC modem

Figure 7.20 Devolo MicroLink dLAN Audio PLC modem

nel) connectors used to broadcast four 192-Kbit/s audio channels over the electrical network.

The audio PLC modems must be configured to parameterize the components of the PLC local area network and to load the plug-ins that the audio file servers require.

PLC can also be used to transmit the telephone analog signal within a building, where only one or two telephone jacks for access to the public STN are usually found. It is then convenient to use the electrical network existing in all the rooms to have telephone jacks remote from the existing jacks.

In this case, two telephone PLC modems are used, one connected to the France Télécom telephone incoming feeder and the other one to an outlet. The analog cellular telephone is connected to the second modem using an RJ-11 connector.

Figure 7.21 illustrates a Wingoline telephone PLC modem used to build a network with 24 modems maximum over the same electrical network. The frequency band used ranges from 3.3 to 8.2 MHz, and the propagation distance over the cables is 150m (slightly lower than that of Ethernet PLC modems).

Figure 7.21 Wingoline telephone PLC modem with two RJ-11 telephone interfaces

Methods for Accessing the Medium

In PLC networks, the method for accessing the medium consists of connecting the PLC devices to the electrical network in order to obtain the best performance at the physical level and the best useful throughput at the upper layer level as a result.

To connect a PLC device to the electrical network, there are two different methods, called "couplings": capacitive coupling and inductive coupling.

The capacitive coupling is the coupling mostly used by PLC modems. The term "capacitive" means that the PLC modem connected to the outlet is viewed as a capacitance (i.e., a capacitor). Figure 7.22 illustrates the operating principle of capacitive coupling.

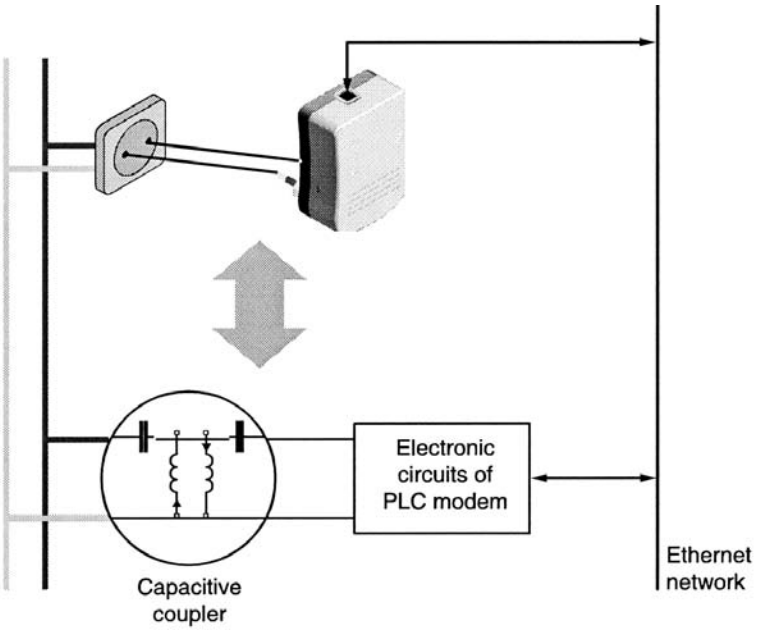

Figure 7.22 Capacitive coupling principle

Coupling

In the electrical field, coupling can be defined as how two electrical circuits connect together in order to generate an electron flow between these two circuits. This electron flow is conveyed by an electric and a magnetic field created between the two electrical circuits due to their inductive and capacitive nature.

Inductive coupling is much more efficient than capacitive coupling. It uses the electromagnetic induction method between two electrical wirings or between an electrical wiring and a coil wound around this wiring. An inductive coupler reduces the attenuation by 10 to 15 dB for some frequencies in comparison with a capacitive coupler. The attenuation between the outlet and the switch box varies from 10 to 30 dB. It is maximum between 15 MHz and 20 MHz.

In the field of PLC networks, the injectors are devices used to connect a PLC device to the electrical network via an inductive coupling directly around electrical wirings, for example, at the level of the electrical switchboard of a building.

Figure 7.23 illustrates the principle of a PLC signal injector consisting of the two following elements:

- A magnetic coil wound around the neutral cable of the electrical network. As we'll see in chapters 11 and 12, the neutral cable is the most interesting cable for the injection of the PLC signal over an electrical network, since it is distributed over all the electrical equipment.
- A cable TV modem connected by a cable (for example, a coaxial cable) to the magnetic coil.

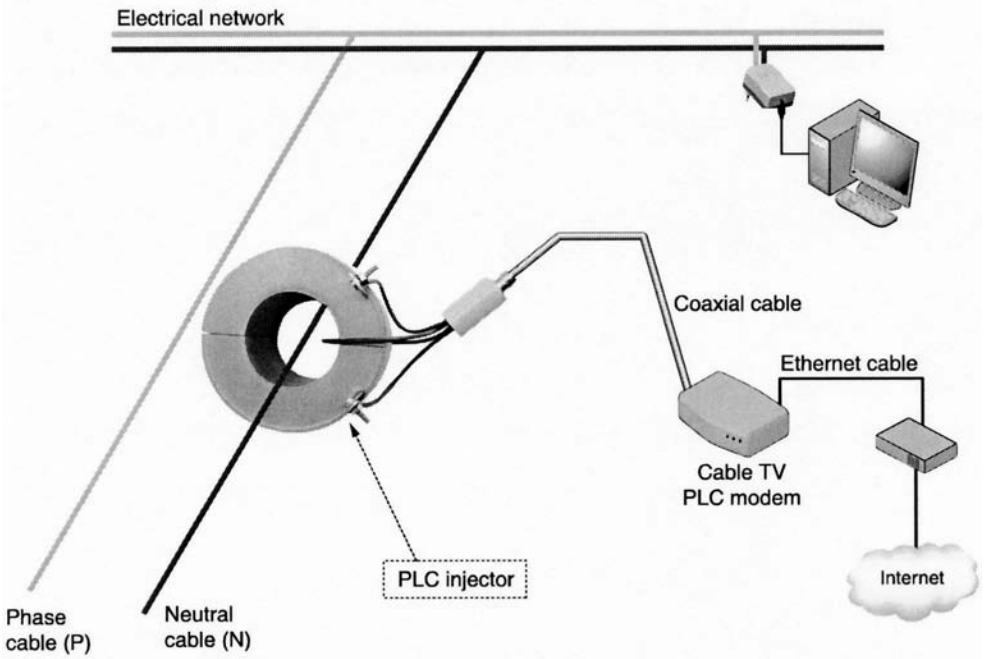

Figure 7.23 PLC signal injection by inductive coupling with a coil over a single-phase network

Figure 7.24 illustrates the same principle but with two magnetic ferrites over a three-phase network.

Choice of Injection Cable

It is preferable to inject the signal over the neutral cable for a single-phase network and on one of the phases for a three-phase network. Better performance is achieved by injecting the signal over a single cable than over several cables at the same time.

This method for connecting PLC devices requires access to the electrical wirings of the 110 to 220V/50 to 60 Hz network, unlike capacitive coupling, which is restricted to the connection of a device to an outlet. Therefore, it is important to request a competent electrician to carry out the coupling operation that requires the knowledge of the electrical hazards close to the cables and components of the electrical network.

Figure 7.25 illustrates an Eichhoff PLC injector with the magnetic coil open (on the left) and closed (in the middle) as it is around the electrical wiring, and the F-type coaxial connector (on the right) used to connect the injector to the cable TV modem.

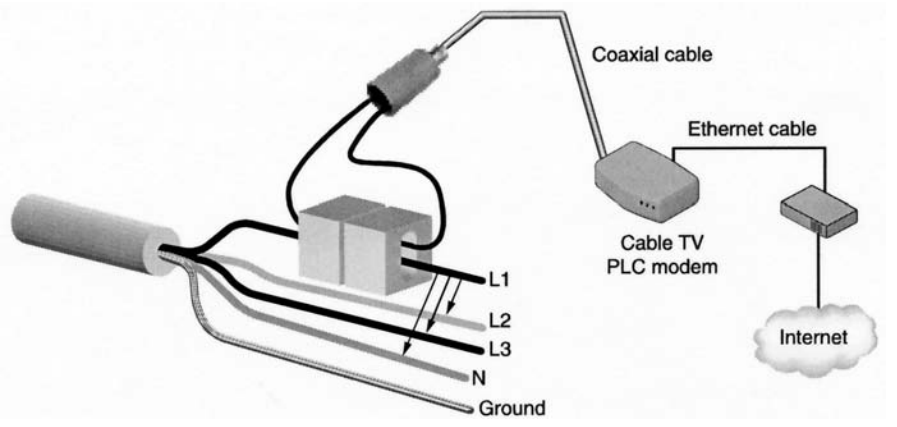

Figure 7.24 PLC signal injection by inductive coupling with two magnetic ferrites over a three-phase network

Figure 7.25 Eichhoff PLC injector with coil and magnetic ferrites

Direct Tap Methods

The "direct tap" methods are used to connect PLC devices directly to the network electrical wirings by perforating the cable insulator and the electrical wiring itself.

Such methods require resorting to an electrician authorized to intervene on LV (low voltage) or MV (medium voltage) electrical networks because of the electrical hazard.

Figure 7.26 illustrates the operating principle of direct tap coupling.

Transformers and Meters

To design the topology of a PLC network, it is necessary to know the range of the PLC signal over the electrical network and to identify the points of the network that may receive this signal. In addition, the PLC network can be secured with this information.

Some devices existing on the electrical network where PLC devices are installed have an influence on the PLC network insofar as they can alter the signal and even cut it off completely. It is then necessary to inject the signal at locations of the electrical network where the PLC signal may not be cut off. Among the devices of an electrical network that may cut off the PLC signal, let's mention the following devices in particular:

- The transformers consisting of two coils used to change the voltage from one value to another one. These coils act as insulators between two parts of an electrical network; this is called "galvanic isolation."

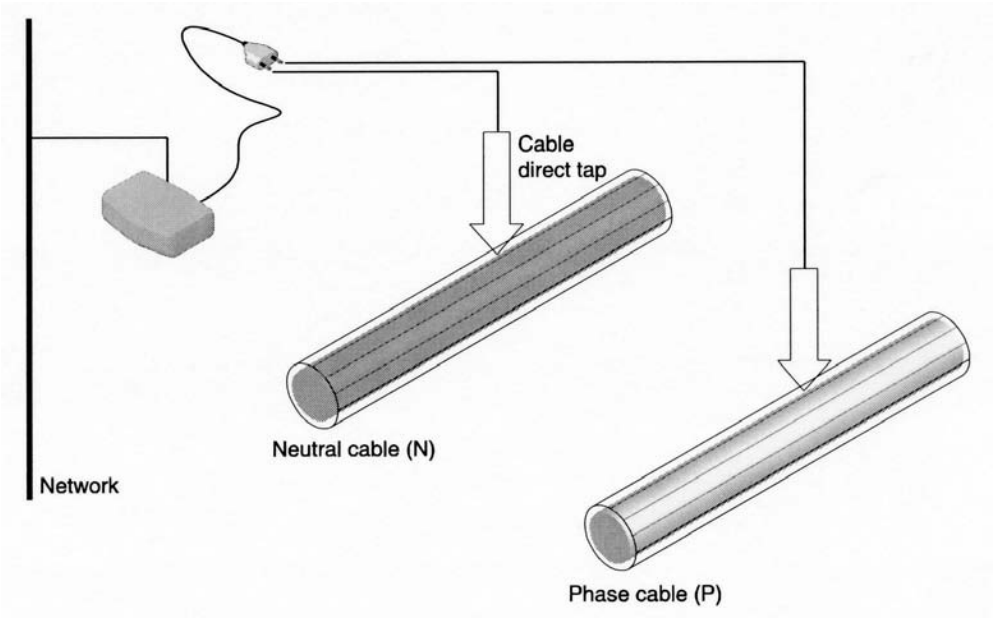

Figure 7.26 PLC direct tap coupling

- Some types of meters integrating a galvanic isolation also behave as PLC signal cutters. However, these models are relatively rare and most meters allow the PLC signal to pass.

In both cases, it may be useful to override these devices to allow the PLC signal to extend over the entire electrical network.

Transformers

Since transformers are inherently electrical devices ensuring a physical isolation between two electrical circuits with a different voltage, they cannot be used to convey the PLC signal between the two parts of the network. In this case, it is necessary to add a PLC device to the transformer; this device is used to retrieve the PLC signal from one side of the transformer and to reinject it on the other side by re-amplifying it so that the signal travels all over the LV electrical network up to the PLC modem of the end user.

Figure 7.27 illustrates the transformer overriding principle with the various PLC signal injection points and the PLC modem of the end user located behind the meter.

A PLC device used to override a transformer can only be installed by teams accredited by the electrical network operator. This is because it is necessary to have access to the MV/LV (medium voltage to low voltage) transformer vault.

Meters

Meters are used to measure the electrical consumption of a house and to invoice the users of the electrical network or of another state-owned electrical company. These

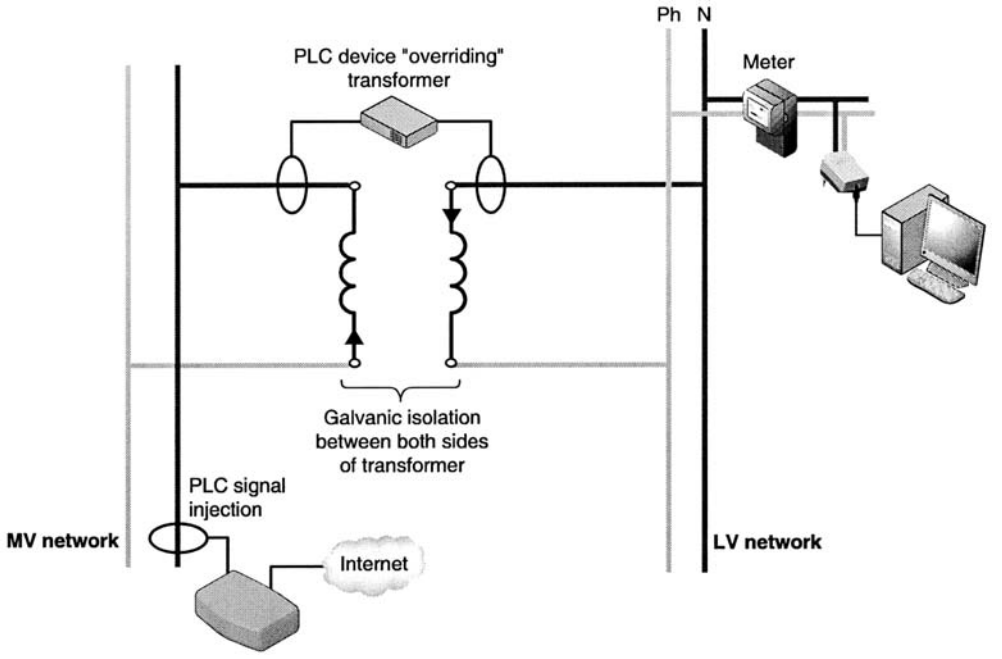

Figure 7.27 Transformer overriding

are major components of an electrical network for the PLC signal since they separate the public electrical network from the electrical network of a building, of an apartment, or of a company.

Most meters allow the PLC signal to pass on each side of the electrical network. Therefore, it is important to correctly configure the PLC local area network encryption if the interception by a malevolent person of data flowing over the electrical network is to be avoided.

Electromechanical meters are the oldest ones. These meters, dating from the seventies, are very frequently encountered in electrical equipment. They allow the PLC signal to pass on either side of the electrical circuit. Their evaluated PLC signal attenuation is 20 dB.

Electromechanical meters were gradually replaced during the 1990s by electronic counters to prevent piracy. These meters, whose piracy is very difficult, are used for remote meter readings via the EDF network using the very low rate, low frequency PLC technology. They also allow the PLC signal to be transmitted. Their evaluated PLC signal attenuation is 15 dB.

Repeaters

Repeaters are devices frequently used in telecommunications to regenerate the data transmission signal when the distances are too long for the received signal to be usable by the data transmission devices.

In the case of PLC networks, the electrical network causes attenuations of the PLC signal (circulation of electrical network components, noises of the connected devices, quality of the electrical wirings, and so forth) that sometimes make it impossible to obtain a PLC link between two distant points of the network without signal repetition.

There are two types of repeaters: passive repeaters and active repeaters. Passive repeaters regenerate the PLC signal by using two PLC chips relaying the signal from one chip to the other one. Repeating takes place both at the physical layer and MAC layer levels. Active repeaters amplify the PLC signal on the electrical wiring without using another PLC chip to relay the signal. Repeating only takes place at the physical layer level.

Figure 7.28 gives an example of repeater use.

Few repeaters can be found in stores since the PLC signal can be satisfactorily broadcast using PLC devices. However, it may be interesting to repeat the PLC signal to obtain suitable bit rates over the entire electrical network.

The following PLC repeaters are available in stores:

- Schneider IR LR 1100;
- Asoka PL8230-2RP (active);
- Oxance PLT300, PLT320 (active);
- CMM RPT1-0.

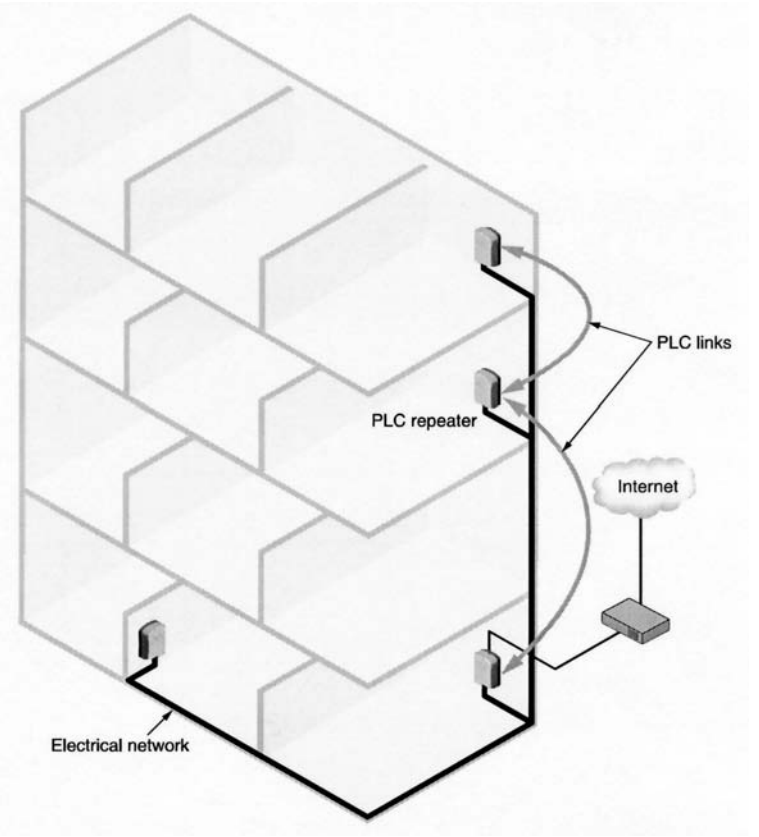

Figure 7.28 Example of PLC repeater use

Home-Made PLC Repeater

A home-made PLC repeater can be fabricated by using Ethernet PLC modems available in stores.

All you have to do is to take two Ethernet PLC modems and connect them with an Ethernet cable (crossover or straight-through cable depending on whether the network interface cards are self-sense cards or not, i.e. that they can adapt or not to network cable crossover). Two different PLC network keys must then be configured on each PLC modem; each key is used by the modem for its connection to a part of the PLC network having the same key (see Chapter 10).

Figure 7.29 illustrates this operating principle.

The two PLC subnetworks communicate between themselves via the repeater consisting of the two Ethernet modems with different encryption keys. However, the disadvantage of this configuration is to reduce the useful throughput of the entire PLC local area network since the repeater uses the frequency band to regenerate the PLC signal on the electrical network.

Filters

As indicated before, the electrical network is a communication medium that may be altered by disturbances originating from the electrical devices connected to it. In par-

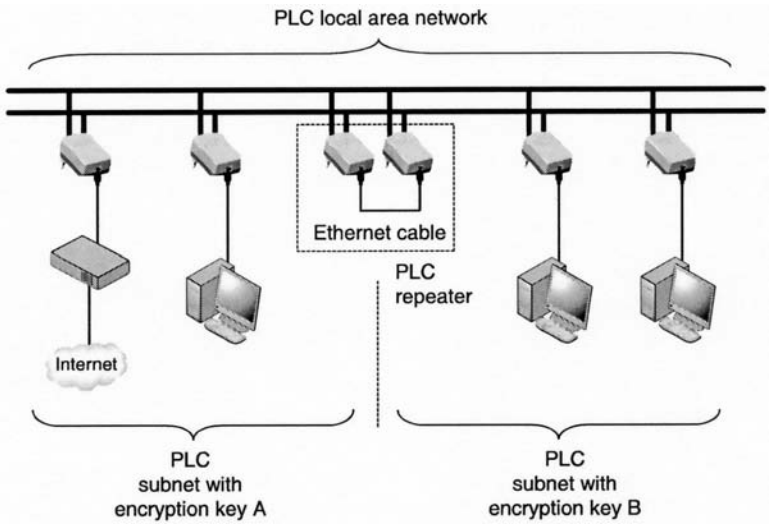

Figure 7.29 Home-made PLC repeater

ticular, these electrical devices send back electromagnetic noises in the frequency band of the PLC devices. Therefore, it is interesting to install filters as close to the disturbing devices as possible in order to stop frequencies generating disturbances.

A PLC filter can also be used to stop the outgoing PLC signal so that it does not propagate outside of the electrical network demarcated by the meter.

Figure 7.30 illustrates an electrical network including PLC devices, disturbing devices (light regulator, hairdryer, power strip, circuit breaker), and the location of the PLC filters.

A filter is connected between the disturbing device and the electrical network. It acts as an over-outlet above the outlet with the disturbing electrical device connecting to the filter.

Table 7.5 summarizes the main electrical devices that may disturb a local area network.

Figure 7.31 illustrates an Eichhoff PLC blocking filter. This device is placed between the electrical switchboard and the domestic, professional or industrial electrical network to prevent the PLC signal from going over the meter and is recovered from another electrical network.

CMM (Courant Multimédia) sells over-outlet antinoise filters that are placed between the potentially disturbing devices of the PLC network and the outlet to which the power supply of the device in question is connected. This device is illustrated in Figure 7.32.

The French PLC company LEA has developed a PLC all-in-one filter and modem to be used on the electrical outlet, filtering the signal coming from the electrical devices connected on this electrical outlet. This device leaves the electrical cable clean from the perturbations coming from the devices connected on a multi-outlet plugged on the Lea NetSocket200+. This device is quite unique in the PLC industry as a whole all-in-one device for filtering, saving an electrical outlet and connecting multiple electrical devices. Figure 7.33 illustrates the Lea NetSocket200+.

Table 7.5 Electrical Devices Disturbing a PLC Network

ELECTRICAL DEVICE	*CAUSE OF DISTURBANCE*
Hairdryer	Motor
Cathode ray tube display	Cathode ray tube
Drilling machine	Motor
Light regulator	Dimmer and Zener diodes
Halogen lamp	Dimmer and Zener diodes
Power strip	Defective electrical connections and accumulation of devices on the same outlet
Device with incorrect CE marking	Outside the disturbance templates

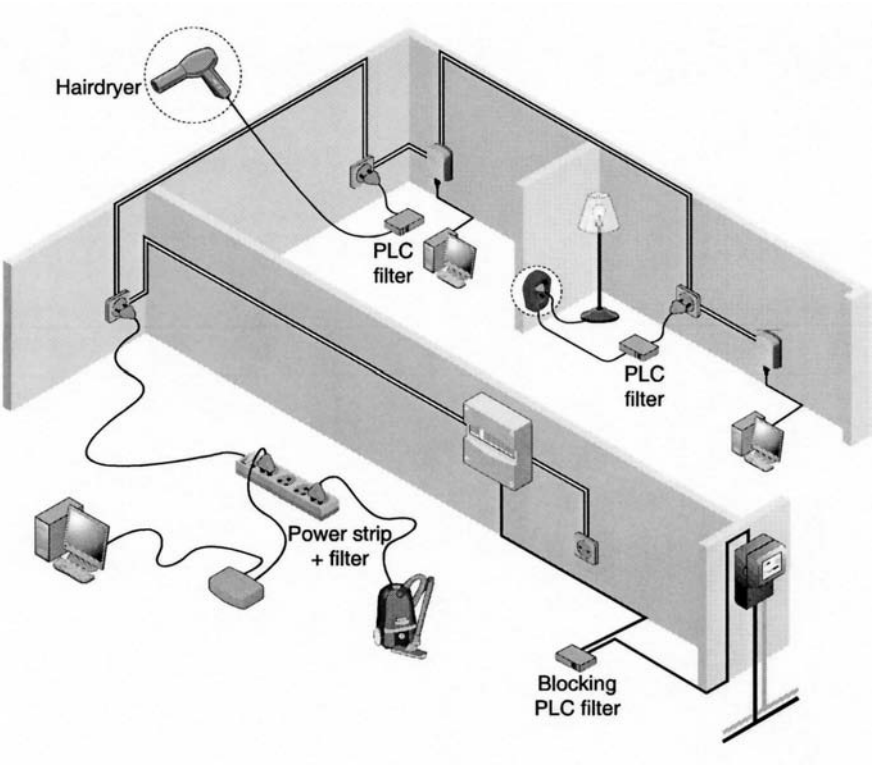

Figure 7.30 Installation of PLC filters on a domestic electrical network

The Cost of PLC

As a result of the evolving HomePlug specifications and increased demand, the prices of PLC products did not stop falling in 2005 and 2006. Between 2003 (date when the first HomePlug 1.0 products were released) and 2005, this fall was on the order of 30%.

Figure 7.31 Eichhoff PLC blocking filter

Figure 7.32 CMM antinoise PLC filter

Figure 7.33 Lea NetSocket200+

The emergence at the beginning of 2006 of HomePlug Turbo products accentuated this fall. We can consider that the price of the HomePlug 1.0 products will still fall by another 20 to 50%.

As soon as the first HomePlug AV products appeared at the end of 2006, the price of HomePlug Turbo products felt in turn by 10 to 20%.

For private individuals, PLCs are an ideal solution to share the same Internet connection between two PCs. Moreover, this is the most usual application of PLC devices. From now on, PLC devices, in particular multi-function PLC modems, integrate all kinds of functionalities and act as Internet modem, router, firewall, DHCP server, switch, and Wi-Fi access point (i.e., six devices in one). If the cost of all these functionalities is taken into account, the price of these PLC devices is after all rather attractive, considering that it is no longer necessary to lay cables or drill holes.

In a company, for the Ethernet cabling of a building, cables must be pulled in all the rooms and telecommunication closets must be installed, which is not the case with PLC. Another advantage of PLC over Ethernet is the dynamic change of topology that it allows. In Ethernet, the topology change generally requires the laying of new cables and results in additional costs.

Table 7.6 summarizes the costs of PLC devices at the end of the first quarter of 2008.

Table 7.6 Costs of PLC Devices

DEVICE	*COST (IN EURO)*
USB modem: – HP 1.0 – Turbo	 50 to 100 80 to 100
Ethernet modem: – HP 1.0 – Turbo – AV	 50 to 100 80 to 100 100 to 300
Cable TV modem	100 to 300
Integrated outlet	100 to 300
PLC/Wi-Fi device	100 to 200
Multi-function PLC device	100 to 300
Audio and telephone PLC device	100 to 150
Inductive injector	120
Repeater	200 to 400
Filter	200 to 400

CHAPTER 8

Installation

The disturbances received and caused by PLC networks must be taken into account when installing the network. The electrical topology of the building or buildings where the devices will be installed is also a major element to be considered for building the architecture of the PLC network.

Therefore, the definition of the electrical network topology is an essential step. It determines the PLC network data transmission performance. PLC devices, whether mobile or fixed on the electrical network, provide various data link qualities depending on their position, the presence of disturbing electrical devices nearby, and the filters installed to protect the electrical network from spurious frequency injections.

Another constraint relates to the actual bit rates since the claimed rates never correspond to what is available to the user. An unexpected lower bit rate generally originates from some mechanisms offered by PLCs. However, this lower bit rate can be minimized by choosing suitable mechanisms and associated parameters when configuring PLC devices and, more especially, the PLC gateway or the central device.

As far as security is concerned, we can see that it is important to implement suitable techniques for data encryption and the separation of logical networks on the electrical network, which can be viewed as a shared data bus. Since the PLC signal's propagation goes via the electrical meters for domestic, professional, or industrial facilities, it is important to use passwords for the PLC local area network that protect data exchanges.

The modeling of an electrical network is difficult and the performance can quickly vary according to the use of PLC devices. This chapter gathers useful information on understanding these variations and improving performance.

Frequency Bands

General public and professional PLCs use two frequency bands: the 3- to 148-kHz frequency band for low rate technologies and the 1- to 30-MHz frequency band for high rate technologies.

PLC technologies for MV (medium voltage) electrical networks, also called BPL (broadband powerLine), may use the 30- to 50-MHz frequency band. These tech-

nologies are installed and implemented under the responsibility of MV electrical network operators.

The 3- to 148-kHz and 1-to 30-MHz bands are called license-free bands, meaning that there is neither a need to ask for authorization nor a need to pay for a subscription in order to use them. However, they are subject to regulation by the ETSI (in Europe) and the FCC (in the USA) which lay down certain restrictions of their use in terms of transmission power.

These bands are divided into sub-bands over which transmissions take place. Insofar as all technologies use these frequency bands, standardization work is in progress so that various PLC systems can coexist on the same electrical network. In Chapter 14, we will once more discuss the coexistence and interoperability of PLC technologies.

Regulation of Radio Frequencies

The issue when deploying telecommunications networks is the achievement of the best possible performance in terms of bit rate, latency, jitter, EMC (electromagnetic compatibility), and coexistence of technologies while complying with the limits laid down by the regulations in force.

Limits on the transmission power and authorized frequency bands are set by these regulations. Rules are also promulgated concerning the acceptable level of disturbances created according to the various radio technologies (amateur radio, analog shortwave, digital radio waves, and so forth).

Due to their technology and medium, PLC devices emit radio waves induced in the electrical wirings conveying the signals.

Unlike Wi-Fi wireless radio networks, PLC devices sold in stores in Europe try to remain within the limits set by Cenélec (European committee for electrotechnical standardization) and ETSI (European Telecommunications Standards Institute). These devices are de facto designed to comply with these limits, and no hardware or software modification is authorized to override them.

The software element of HomePlug devices does not give access to any hardware parameters (carrier frequency, frequency sub-bands, or transmission power). This means that the Ethernet frames sent by the configuration tools of PLC devices (see Chapter 10) cannot be used to modify the frequencies and power used by the devices. Therefore, for the PLC network user, the configuration does not give access to the physical layer's parameters, unlike Wi-Fi, with its 11 channels and its parameterization of the interface transmission power.

Figure 8.1 illustrates the sending of a frame by the configuration tool to the PLC device to be configured. This frame is a conventional Ethernet frame recognizable on a network with its ETHERTYPE field, which, in its data, contains the parameters to be configured so that the PLC network can operate in the best way possible.

The frequency utilization spectrum defined by the ETSI is globally broken down as illustrated in Figure 8.2. Referring to the rules promulgated by the regulatory authorities, it gives an idea on the distribution of general public radio frequencies close to those used by the various PLC technologies.

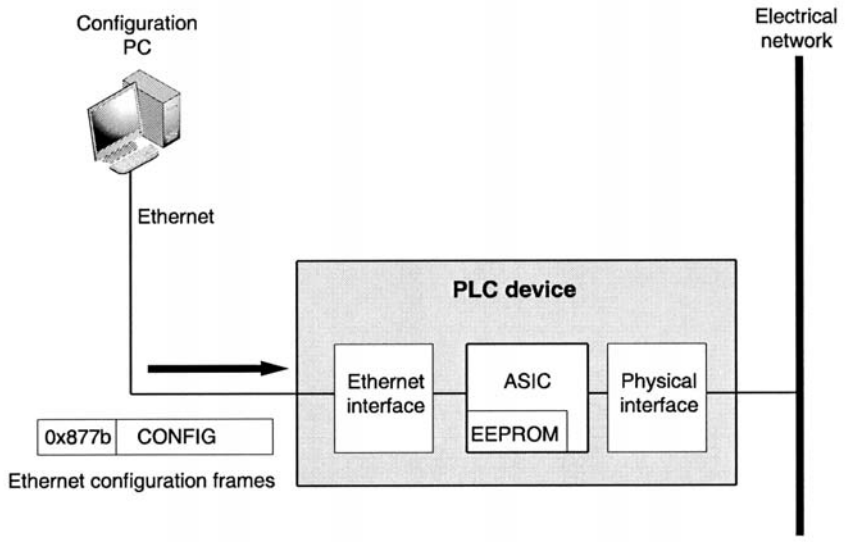

Figure 8.1 Ethernet frame for the configuration of a HomePlug network

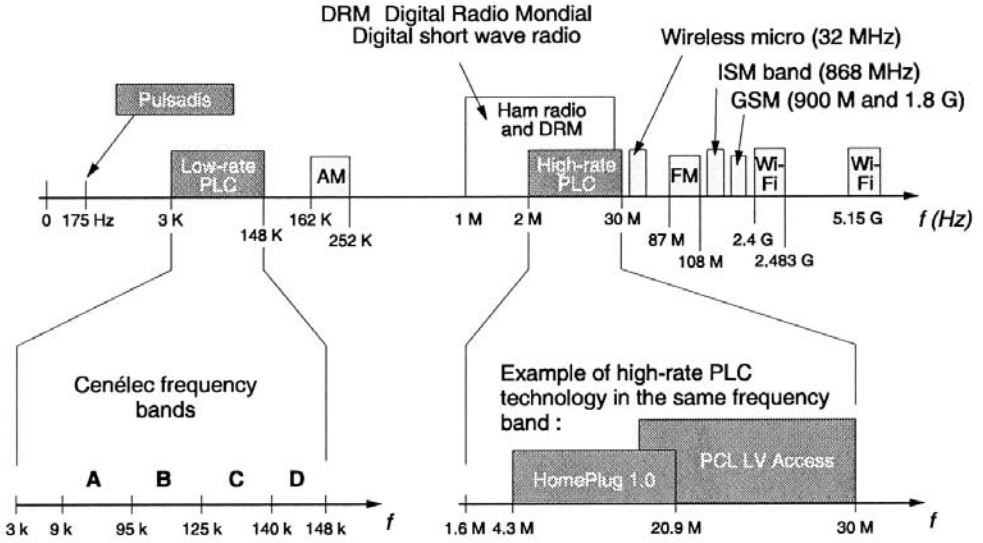

Figure 8.2 PLC frequency bands

As explained before, the PLC networks are not radio networks, but their implementation over electrical wiring produces radiated waves that propagate with the wiring acting as radio aerials. Therefore, PLC networks are viewed by the telecommunications regulatory bodies as radio networks that, as such, must comply with transmission power and frequency band constraints.

As indicated before, the frequencies used by high rate PLC are within the 1- to 30-MHz band. This band is also used by amateur radio and future digital short-wave radio called DRM (Digital Radio Mondial), which will be used to

broadcast digital quality radio programs over very long-range links and also to transfer data at rates of some tens of kilobits/s.

The disturbances caused by PLC networks for amateur radio operators and the DRM have been the subject of many discussions to make it possible for various technologies to coexist. These discussions have led the developers of PLC technologies to include filtering techniques for frequencies already used by other radio technologies. These techniques, called "notching," consist of listening to the radio channels to readjust or take away some frequencies.

Dynamic Notching of Frequency Bands

As illustrated in Figure 8.3, when the PLC network notices that the f1 and f2 frequencies are used, it takes away the frequency bands containing f1 and f2 in its authorized spectrum. These frequency bands are still off throughout the use of f1 and f2, then on again as soon as these frequencies are no longer used.

This dynamic technique is based on listening to the signal-to-noise level measured in dB for each frequency band.

Low Bit Rate PLC

Mainly used in home automation and car automation (industrial bus of automotive vehicles), the frequencies authorized for low bit rate PLC are described by the Cenélec in the EN-50065-1 standard. This standard defines the utilization characteristics of all the frequency bands between 3 kHz and 148 kHz. The PLC signal transmission power is limited by the maximum permitted voltage, which is 3.5V for these frequency bands.

Table 8.1 summarizes the characteristics of low bit rate PLC frequency bands.

As a reminder, the AM radio band covers the 162 to 252 kHz spectrum.

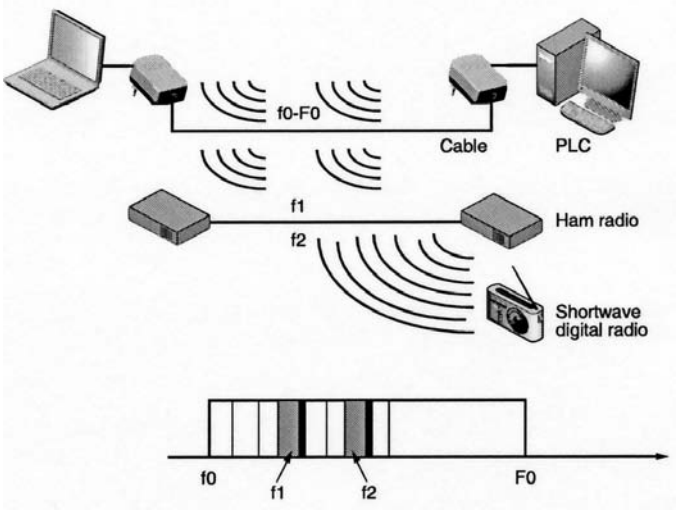

Figure 8.3 Notching of congested frequencies

Table 8.1 Cenélec Frequency Bands for Low Bit Rate PLC

CENÉLEC BAND	*FREQUENCY BAND*	*USE*
	3 to 9 kHz	Limited to electrical network operators for their specific needs, like remote meter reading
A	9 to 95 kHz	Limited to electrical network operators
B	95 to 125 kHz	Home automation use (baby phones, and so forth)
C	125 to 140 kHz	Home automation use (X10, and so forth)
D	140 to 148 kHz	Home automation use

Particular Case of EDF Pulsadis Signal (France) for Day/Night Tariff Meters

The Pulsadis signal is better known as the day-night signal, since it is used by EDF meters in France to switch over a number of energized devices during the night to benefit from EJP tariffs or EDP timers. This signal is sent over the EDF electrical distribution network at the frequency of 175 Hz.

Figure 8.4 illustrates the electrical architecture of an LV electrical network with implementation of the Pulsadis signal from EDF monitoring stations to the subscriber's meter.

Once received by EDF day/night tariff meters, this signal triggers the contactors of duly fitted electrical devices at the domestic circuit breaker panel. For instance, this makes it possible to turn on water heaters during the night before switching back to full rate at 7 a.m.

This is a low frequency signal that enables its good propagation over the electrical network. Its 175-Hz frequency is different from 50 Hz and its related harmonics (100 Hz, 300 Hz, 600 Hz, and so forth). The signal consists of one-second binary pulses spaced out by one and a half seconds. This is a 102.25-second frame.

High Bit Rate PLC

The 1- to 30-MHz frequency band of high bit rate PLCs is more or less used. It is generally viewed as consisting of two sub-bands, a 1- to 20-MHz lower band, which is especially used in domestic usage internal PLC, and a 2-to 30-MHz upper band, which is especially reserved for medium voltage electrical network public usage external PLC.

As far as domestic usage internal PLC are concerned, the various technologies used, which are all based on OFDM, share the frequency band differently to achieve the best possible performance in terms of bit rate and latency. This performance is obtained by constantly improving the physical layer (PHY), data link layer, and MAC layer modulation techniques including their methods for access to the physical medium.

HomePlug 1.0 uses the 4.49 to 20.7-MHz band and 84 sub-carriers with division of the 0 to 25 MHz frequency band into 128 bands of 195,3125 kHz. In this way, if each band is numbered from 1 to 128, HomePlug 1.0 uses bands 23 to 106.

In the United States, some bands 23 to 106 are used by ham radio operators (17m, 20m, 30m, 40m). Therefore, eight bands corresponding to the frequencies of

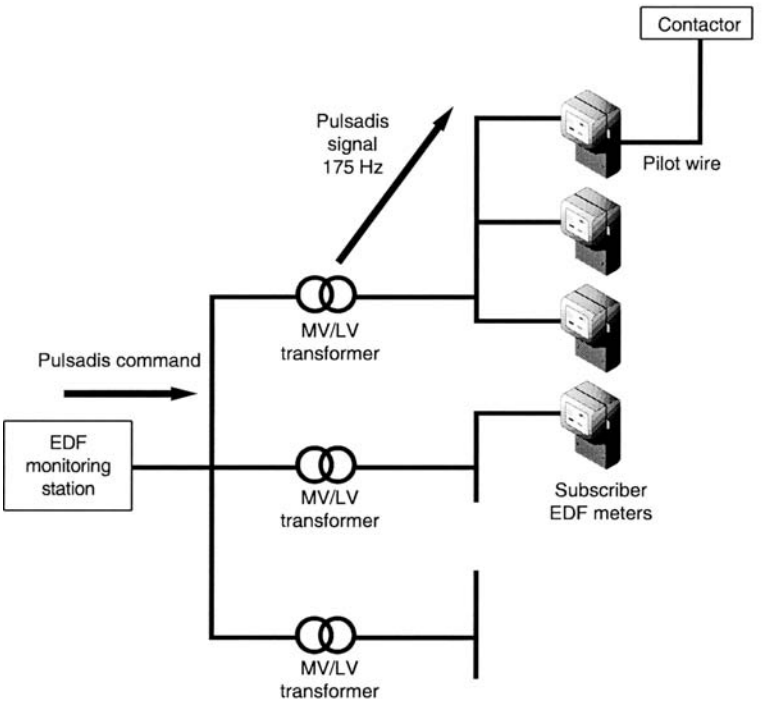

Figure 8.4 Architecture for Pulsadis signal implementation over the EDF LV electrical network

ham radio operators are not used. The total HomePlug 1.0 bands are therefore equal to de 84 – 8 = 76.

Table 8.2 summarizes the high rate frequency bands which can be used according to each type of PLC technology.

Since the 1- to 30-MHz frequency band is divided into sub-bands, each sub-band conveys the OFDM modulation carriers at the transmission channel level. Therefore, and unlike Wi-Fi, there are no channels, strictly speaking, which could be configured to build the network architecture. In PLCs, the entire frequency band is used as the transmission channel; all sub-bands are used for improved transmission robustness.

Table 8.2 Frequency Bands of High Rate PLC Technologies

PLC TECHNOLOGY	*FREQUENCY BAND*	*OFDM CARRIER NUMBER*
HomePlug 1.0	4.49 to 20.7 MHz	76
HomePlug 1.1	Same	Same
HomePlug AV	2-28 MHz	917
DS2 –45 Mbit/s –200 Mbit/s	–1.6 to 30 MHz –2.46 to 11.725 MHz + 13.8 to 22.8 MHz	–100 –1,280 + 1,280
Spidcom	–2 to 30 MHz –30 to 60 MHz (external)	–900 –Same
Main.net	4.3 to 13 MHz	NC

In addition, and unlike Wi-Fi, the network configuration does not require you to make choices according to the other assigned channels. All the channels of the permitted bands, called "sub-bands" are used. Therefore, the network can be congested by the various technologies coexisting on the same electrical network. In this case, free or infrequently used sub-bands are used by PLC technology. In Chapter 13, we'll examine the coexistence of PLC technologies and the work in progress on an interoperability standard.

Figure 8.5 illustrates the frequency domain of the various PLC modulation OFDM sub-bands and the associated binary data in the case of a HomePlug 1.0 PLC network.

Electromagnetic Compatibility and Frequency Bands

The various electrical and electronic devices that we use within a domestic, professional, or industrial background produce radio electromagnetic emissions in the environment close to where they operate.

The frequencies of these radio electromagnetic devices may interfere with the operation of the network's PLC devices and prevent data communications in frequency sub-bands. Some devices produce more disturbances than other devices on PLC networks. For example, the CE marking in force in the European Community stipulates the limits for the radioelectromagnetic emissions of electrical and electronic devices sold in stores.

Chapter 7 (see Table 7.7) gives a list of PLC network disturbing devices. We'll examine this a bit further in this chapter about interference.

Reciprocally, PLC devices emit electromagnetic waves that may interfere with the operation of the surrounding telecommunications devices around the electrical wirings. The CISPR (international special committee on radio interference) of the IEC (International Electrotechnical Commission) indicates wave emission limits for PLC devices.

Current PLC technologies, such as HomePlug AV, implement a notching technique in order to comply with these emission constraints.

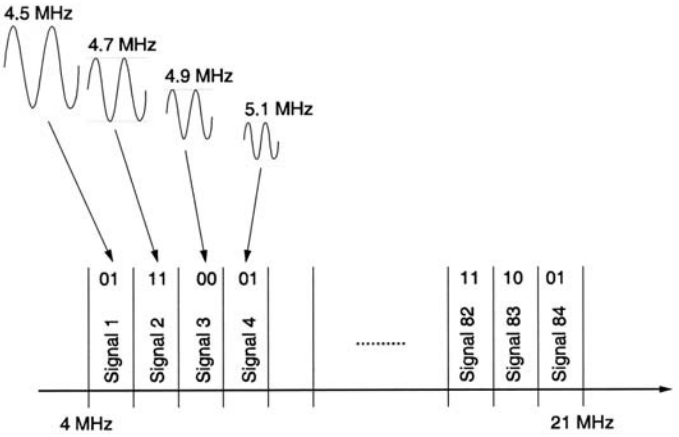

Figure 8.5 HomePlug 1.0 PLC modulation OFDM sub-bands

Figure 8.6 shows that the transmission channel can be viewed as N sub-bands with their sub-carriers, all of them operating simultaneously and each conveying part of the physical layer data.

Transmission Power of PLC Devices

The measured power of the signal emitted by marketed PLC devices is usually 20 dBm (measured in the 1 to 30 MHz band).

The power can be expressed by variables P or G:

$$P = 10^{G/10} \text{ and } G = 10 \log P$$

where G corresponds to the gain (in dBm or dBi) and P to the power (in mW).

Table 8.3 gives the correspondence between the power and the gain.

Since the power limit is set to 100 mW (equivalent to 20 dBm measured in the 1- to 30-MHz band) for the electrical networks' PLC devices, the performance of the transmission channels depends on the signal range.

To be in line with the regulations in terms of EMC (electromagnetic compatibility) laid down by the CISPR committee, PLC devices must limit their transmission power. This transmission power is measured as a quasipeak value, and not as a mean value. In the frequency domain, this corresponds to a PSD (power spectral density), i.e., a uniform distribution of the total transmission power on all the frequency sub-bands of the 1- to 30-MHz band.

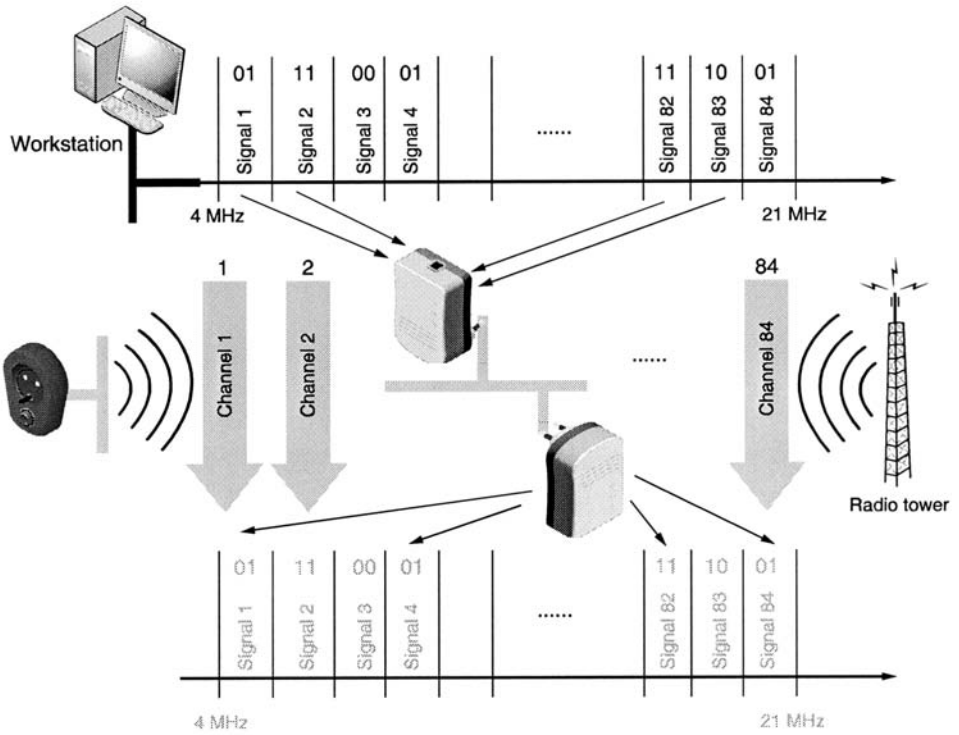

Figure 8.6 PLC technology multichannel OFDM modulation

Table 8.3 Gain/Power Correspondence

GAIN (IN dBm)	*POWER (IN mW)*
3	2
5	3.1
7	5
9	8
15	31.6
19	79.4
24	251.1

The HomePlug 1.0 technology includes 84 sub-bands of 195.31 kHz, whereas HomePlug AV comprises 918 narrower sub-bands of 24.414 kHz. Therefore, the PSD wave is less important in HomePlug AV, which makes it possible to increase the transmission power by 2.2 dB for PPDU data.

Figure 8.7 illustrates the PSD deviation between HomePlug 1.0 and AV. The PSD is expressed in dBm/Hz.

Table 8.4 summarizes the mean transmission power of the various components of the HomePlug's physical frame in these two versions.

The HomePlug 1.0 and AV specifications stipulate that, in order to comply with the EM (electromagnetic) emission limits, the PSD of PLC devices must be equal to or less than –50 dBm/Hz.

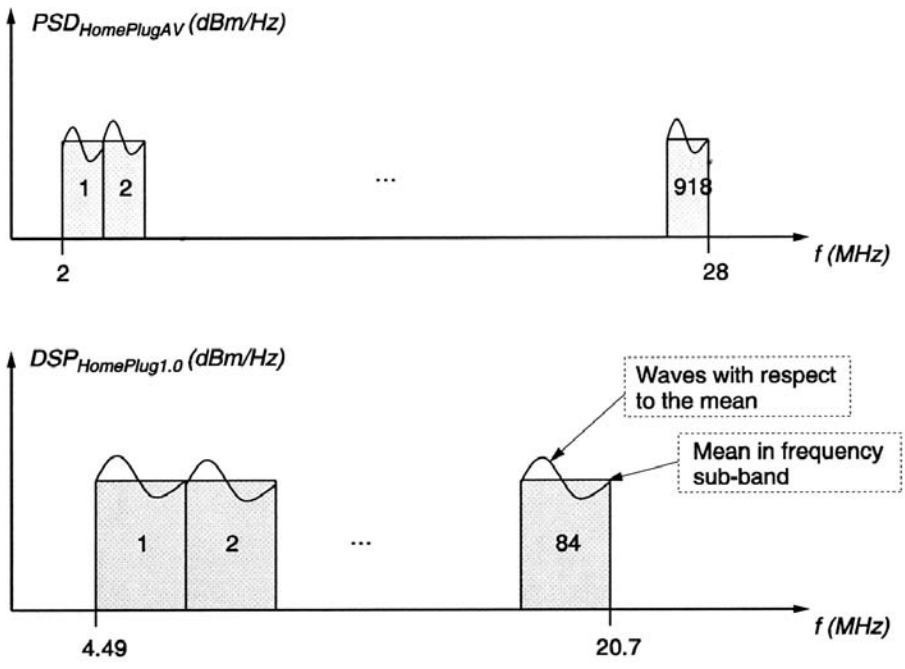

Figure 8.7 PSD differences between HomePlug 1.0 (top) and HomePlug AV (bottom)

Table 8.4 Transmission Power in Each Sub-Band

PHYSICAL FRAME COMPONENT	*AVERAGE TRANSMISSION POWER*	
	HomePlug 1.0.1	HomePlug AV
Preamble	3 dB	3 dB
FC (Frame Control)	0 dB	3 dB
PPDU data	0 dB	2.2 dB
PRS (Priority Resolution Symbol)	3 dB	3 dB

Figure 8.8 illustrates the HomePlug AV PSD curve in the 1- to 30-MHz band. We clearly observe that some frequencies are less emissive than other ones (–80 dB in comparison with –50 Hz). We can consider that a frequency, the PSD of which is around –80 dB, is not perceptible for the electrical network and the devices close to electrical wiring.

Table 8.5 summarizes the various HomePlug AV sub-bands, from 1.71 to 28 MHz, with their maximum PSD (expressed in dBm/Hz) and whether the sub-band is active or not (if another technology already uses this sub-band), with the numbers of sub-bands 0 to 1,535. The last column gives the radio technologies in this sub-band.

Topology of Electrical Networks

There are two wiring types for the electrical networks of any building, whether domestic, professional, or industrial:

- *Single-phase,* consisting of two cables (neutral and phase). The electrical potential difference between these two cables is 110V or 220V flowing from the circuit breaker panel to the outlets and lights of the building.
- *Three-phase,* consisting of four cables (neutral and three phases). The electrical potential difference between the neutral cable and a phase cable is 110V or

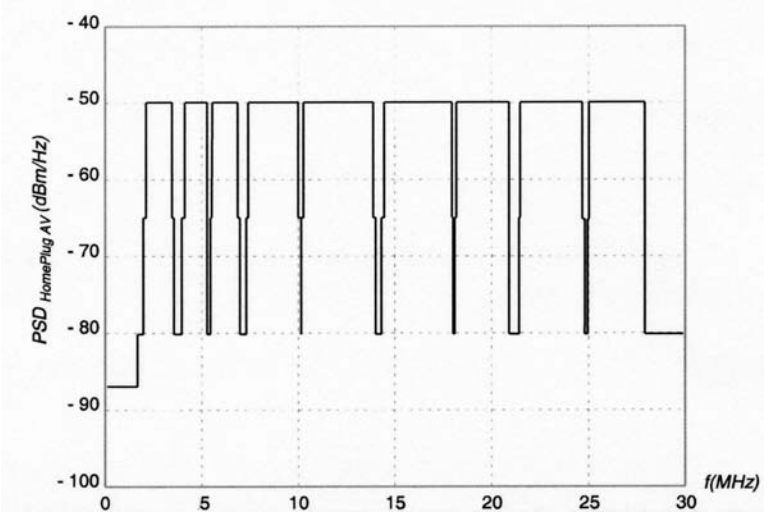

Figure 8.8 Limit PSD mask for HomePlug AV in the 1- to 30-MHz frequency band

Table 8.5 PSD and Regulations in Each HomePlug AV Sub-Band

CENTRAL SUB-BAND FREQUENCY (MHz)	*MAX. PSD (dBm/Hz)*	*CARRIER ON/OFF*	*COMMENT*
F ≤ 1.71	–87	Carriers 0–70 off	AM broadcast band and below
1.71 < F < 1.8	–80	Carriers 71–73 off	Between AM band and 160m amateur band
1.8 ≤ F ≤ 2	–80	Carriers 74–85 off	160m amateur band
2 < F < 3.5	–50	Carriers 86–139 on	HomePlug carriers
3.5 ≤ F ≤ 4	–80	Carriers 140–167 off	80m amateur band
4 < F < 5.33	-50	Carriers 168–214 on	HomePlug carriers
5.33 ≤ F ≤ 5.407	–80	Carriers 215–225 off	5 MHz amateur band
5.407 < F < 7	–50	Carriers 226–282 on	HomePlug carriers
7 ≤ F ≤ 7.3	–80	Carriers 283–302 off	40m amateur band
7.3 < F < 10.10	–50	Carriers 303–409 on	HomePlug carriers
10.10 ≤ F ≤ 10.15	–80	Carriers 410–419 off	30m amateur band
10.15 < F < 14	–50	Carriers 420–569 on	HomePlug carriers
14 ≤ F ≤ 14.35	–80	Carriers 570–591 off	20m amateur band
14.35 < F < 18.068	–50	Carriers 592–736 on	HomePlug carriers
18.068 ≤ F ≤ 18.168	–80	Carriers 737–748 off	17m amateur band
18.168 < F < 21	–50	Carriers 749–856 on	HomePlug carriers
21 ≤ F ≤ 21.45	–80	Carriers 857–882 off	15m amateur band
21.45 < F < 24.89	–50	Carriers 883–1,015 on	HomePlug carriers
24.89 ≤ F ≤ 24.99	–80	Carriers 1,016–1,027 off	12m amateur band
24.99 < F < 28	–50	Carriers 1,028–1,143 on	HomePlug carriers
F ≤ 28	–80	Carriers 1,144–1,535 off	10m amateur band

220V and is 190V or 380V between two phase cables. A three-phase electrical network rather than a single-phase network is used in some buildings since it makes it possible to convey more electrical power and therefore to supply more electrical devices in the building. Three-phase networks are also used to supply motors requiring a three-phase voltage for their operation.

Both topologies are described more precisely in the following sections.

Single-Phase Wiring

Most dwellings (apartment, house, small building) have single-phase wirings, since their electrical power supply requirements are less than a 60-A current.

As illustrated by Figure 8.9, a single-phase electrical wiring includes several cables (bus-bar connections) starting from the circuit breaker panel to supply power to the home's electrical devices and lights.

Figure 8.10 illustrates the topology of the single-phase electrical network of an apartment with the various cables starting from the circuit breaker panel. The PLC devices and modems connect to the outlets of the house rooms. The PLC signal

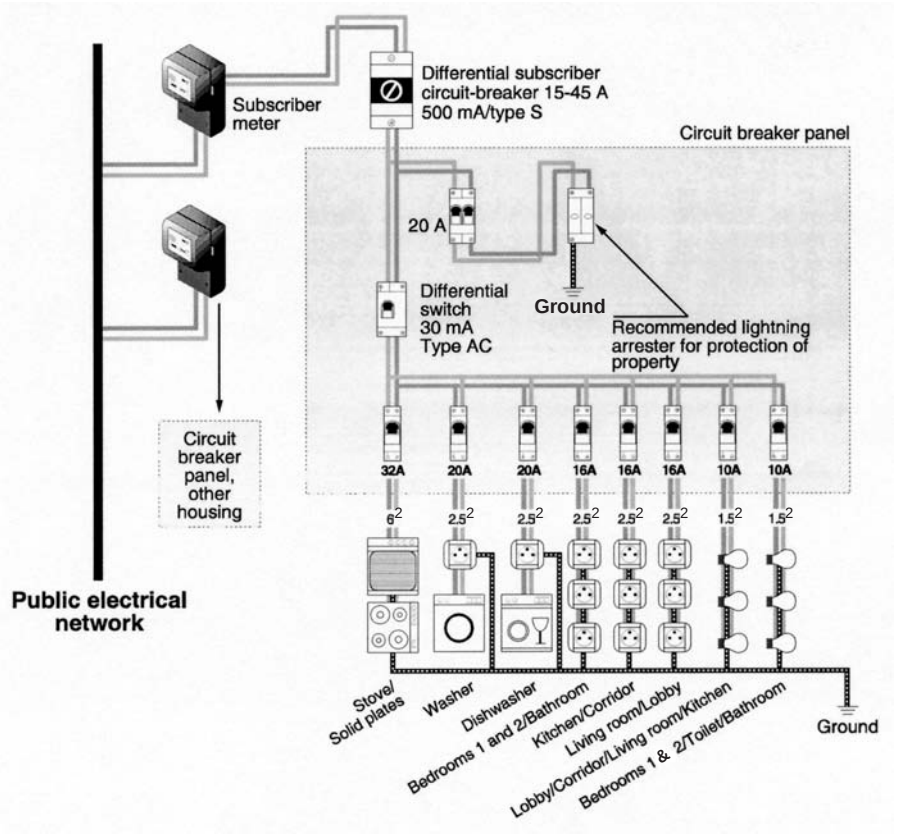

Figure 8.9 Topology of a domestic single-phase electrical network

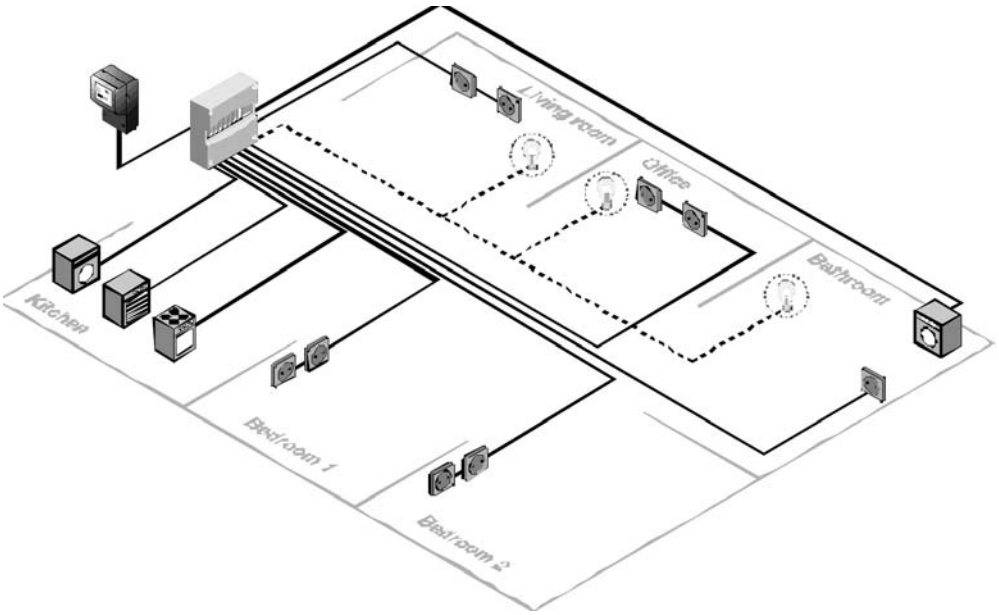

Figure 8.10 Topology of an apartment single-phase electrical network

propagates over the cables then goes via the circuit breaker panel to start at the various cables again. The wiring length can exceed 300m, which is considered as the acceptable limit for a satisfactory useful throughput.

The electrical devices connected to the network are potential sources of electromagnetic disturbances for the PLC signal. Remember that the average length of the electrical wiring between the switchboard and the farthest outlet should not exceed 200m.

Three-Phase Wiring

Buildings, large houses, professional premises, or plants have greater electrical power requirements than a domestic dwelling; therefore, the electrical network is often a three-phase network in them.

Four cables (neutral, phases 1, 2, and 3) start from the circuit breaker panel and supply the outlets of the building. Figure 8.11 illustrates an example of three- phase wiring in a building with several stories with the various electrical phases supplying the building stories. Two cables starting from the switchboard travel all over each story: a phase cable and the neutral cable.

The single cable that is common to the entire building is the neutral cable. The other cables are electrically dissociated. It is important to remember that the PLC signal flowing in one of the cables (neutral or phase cable) can be transmitted in the other cables due to an induction phenomenon. This makes it possible to build the topology of the PLC local area network by making optimal use of the properties of the electrical wirings.

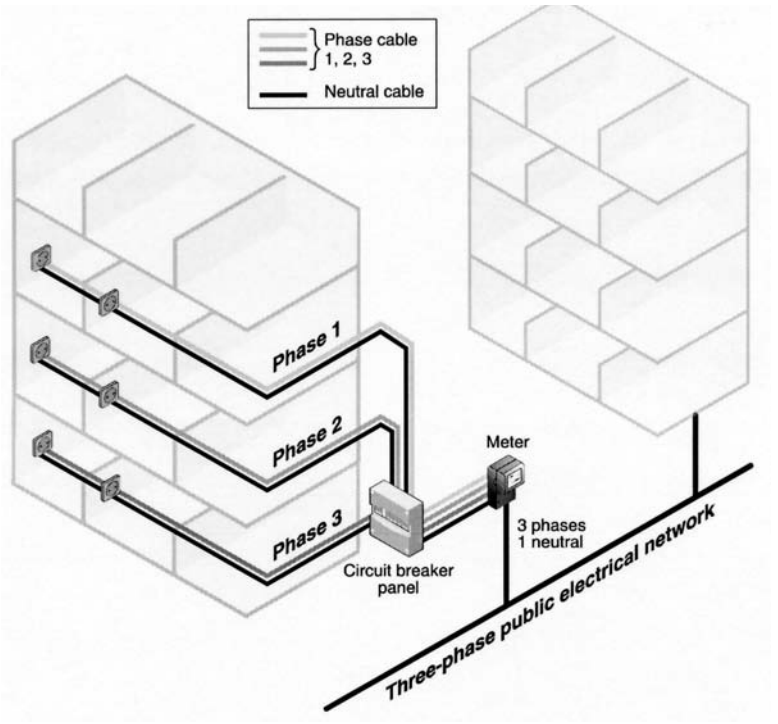

Figure 8.11 Topology of a three-phase electrical network for a large building

Like for single-phase networks, the average distance between the circuit breaker panel and the last outlet connected to the electrical wiring must not exceed 200m. If the PLC signal flows over the cables, goes through the circuit breaker panel, and propagates over other cables again, then distance is greater than 200m, and the useful throughput may fall.

The PLC signal also goes through the meter and may reach the electrical network of the adjacent building, which can turn out to be useful if building a PLC local area network between buildings is desired. However, this requires good security for the PLC signal to avoid listening to the PLC network.

Wiring in an Electrical Network

The signal propagation may be affected by the cable section. To simplify, we can say that the higher the cable section, the higher its attenuation.

Table 8.6 summarizes the various cable sections between the utility meter and the circuit breaker panel.

Table 8.7 lists the recommended electrical conductor sections according to the function of the device connected to this cable (NFC 15-100 standard). Therefore, the cable sections that are mainly used are 1.5 mm² or 2.5 mm².

The Circuit Breaker Panel

The circuit breaker panel is the heart of the electrical network, from which all the electrical wirings start. This panel is also the component protecting people from

Table 8.6 EDF Connection Cable Section According to Delivered Power

RATED CURRENT OF SERVICE SWITCH	*MINIMUM SECTION OF COPPER CONDUCTORS*
45A	10 mm^2
60A	16 mm^2
90A	25 mm^2

Table 8.7 Sections of Conducting Cables According to Electrical Devices

FUNCTION	*SECTION (mm^2) OF COPPER CONDUCTORS (Ph, N, T)*	
Standard	*NFC 15-100 standard*	
Lighting and controlled outlet	8	1.5
Outlet	8	2.5
Washer	1	2.5
Stove (oven + plate) or solid plate	1	6
Oven alone	1	2.5
Two hobs (studio)	1	2.5
Thermal storage water heater	1	2.5
Heating: convector, panel heater	5	1.5 mm^2 minimum

electrical hazards. The protecting devices are called "circuit breakers" (or fuses for old networks). They may be of several types. Each circuit breaker has specific characteristics concerning the attenuation of the PLC signal conveyed over the cable.

Figure 8.12 illustrates an example of a closed (on the left), open (in the middle), and front elevation (on the right) circuit breaker panel. The devices connected to the panel are identified in it.

Attenuation on an Electrical Network

We have seen that, beyond a linear length of 300m (in a wound electrical cable, the self-induction phenomenon does not give the same results), the useful throughput quickly falls, due to the signal attenuation, to such an extent that it becomes too low to offer a satisfactory quality of service for upper layer applications.

Each cable has a different section and impedance characteristics inducing different PLC signal attenuations. At 100m, the attenuation of the HNS33S33 cable used in LV public networks is 14 dB for a PLC signal at the frequency of 30 MHz.

There are several types of electrical wirings for an LV (low voltage) installation in a building:

- Cables called *conductors, phase, neutral,* and *ground* are placed in the walls or in individual sheaths but are not grouped in one single sheath. This wiring type induces a higher electromagnetic emission in the immediate environment. Due to the loss of these electromagnetic emissions, the PLC signal propagation over the cables is subjected to a rather high attenuation. These cables are typically found in installations under the H07 V-U or H07 V-R (rigid conductors), H07 V-K (flexible conductors), P/N for conduit, molding, or plinth mountings.
- P, N, and G cables are installed together in a twisted way with the ground cable in the middle of the twist inside a sheath. A much better propagation of the PLC signal is achieved with this type of cable since the cables induce electromagnetic couplings between themselves. In addition, just like the telephone cable, the twisted arrangement allows better guidance of the PLC signal and makes it possible to avoid attenuations caused by electromagnetic leakage in the immediate environment. The signal is still relatively confined in the sheath and achieves better performance, with respect both to the distance and bit rate. These cables are typically found in installations under FR-N 05 VV-U or R (rigid cables), A05 VV-F or H07 RNF (flexible cables), P/N for surface mountings, in air spaces, moldings, plinths, or conduits.
- P, N, and G cables are twisted together by the electrical installer before placing them in raceways or in the building walls. This wiring type provides a good propagation of the PLC signal and very little loss due to electromagnetic emissions.

Recommended Cable Length in an Average Domestic Installation

If we take the case of an average house (i.e., a 100-m² F4 single-story house or a 65-m² T3-T4 apartment), the general cable length between the circuit breaker panel and the out-

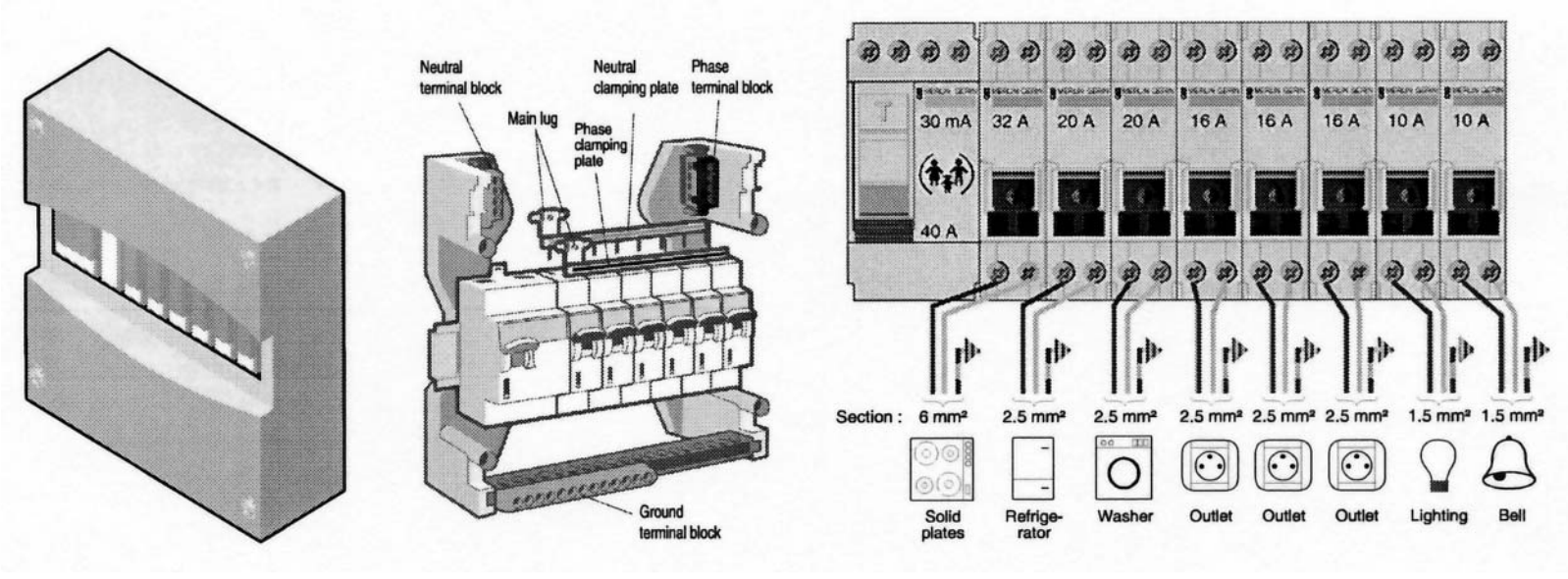

Figure 8.12 Circuit breaker panel of a domestic installation

lets is 15m. The maximum cable length between the circuit breaker panel and the farthest point (luminous point or outlet) generally is 50m.

It is important to limit the voltage drop in the electrical cables to 2% to keep an acceptable voltage for the electrical devices connected to the installation network.

The following formula is used to determine the corresponding single-phase cable length:

$$L = \Delta_u \times \frac{U_0}{100} \times \frac{1}{2\rho} \times \frac{S}{I} \text{ (length expressed in meters)}$$

where

Δ_u is the voltage drop as a percentage.

U_0 is the voltage of the electrical network (110V or 230V).

ρ is the resistiveness of the electrical wiring (0.023 for copper and 0.037 for aluminum).

S is the cable section in mm².

I is the strength of the current flowing through the cable, expressed in A.

For a copper single-phase cable with a voltage drop of 2%, this formula becomes:

$$L = 100 \times \frac{S}{I}$$

For a cable supplying luminous points with a 1.5-mm² section and a maximum permitted current of 16A, it is recommended to have a cable length of 9.3m. For a cable supplying outlets with a 2.5-mm section and maximum permitted current of 20A, it is recommended to have a cable length of 12.5m.

Choosing the Topology for a PLC Network

The PLC local area network must adapt to the electrical network of the building. Each building can have various types of cables, various circuit breaker panels, various circuit breakers, various cut-out switches (fuses, circuit breakers), and also circuit components connected in series (outlets connected in series to the electrical wiring) or in parallel (outlets directly connected to cables from the circuit breaker panel).

In the same manner as a Wi-Fi network must adapt to the structure of the walls of a building, which act as many obstacles to the propagation of radio waves, a PLC network must adapt to the electrical network and to raceways, which act as obstacles to the propagation of the PLC signal.

The topology of the PLC local area network must adapt to that of the electrical network in one or several of the following ways:

- Insofar as possible, determine the topology of the electrical network, for example by recovering the network diagram or by performing PLC tests on the various outlets of the building.
- Find the best points for the connection of PLC devices to the electrical network in order to achieve the best possible PLC coverage. The circuit breaker panel is a central point for the electrical network since all the electrical wirings originate from it.

- Identify the areas of the electrical network where the PLC signal is not received and the parts of the building connected to other electrical networks or through various outlets revealing excessive cable lengths or subjected to too many disturbances.

We'll examine this topology choice again in Chapters 11 and 12.

Propagation of the PLC Signal

One of the recurrent problems with the PLC technology is the signal propagation over electrical wirings. Since these wirings have a specific resistiveness, the signal propagation is subjected to an attenuation proportional to the cable length.

The tests performed by PLC device manufacturers and telecommunications test laboratories, as well as feedback from deployed PLC networks, are used to set some Figures relating to the PLC signal propagation.

"Internal" cables are cables used in private electrical networks (i.e. in domestic, professional, and industrial buildings). The signal attenuation according to the cable length can be evaluated with the various measurements carried out on copper electrical wirings of 1.5 and 2.5 mm diameters.

Figure 8.13 illustrates the results of these tests at three significant frequencies: 10 MHz, 20 MHz, and 30 MHz. We notice that the attenuation is higher for higher frequencies of the 1 to 30-MHz band. Since the cable length of a domestic installation is 200m on average, the PLC signal attenuation allows for the maintaining of data exchanges, since the devices use interfaces that are sensitive enough to receive the signal.

"External" cables are cables that belong to the public electrical network of the utility. These cables are of the three-phase LV or MV type and are either buried, and

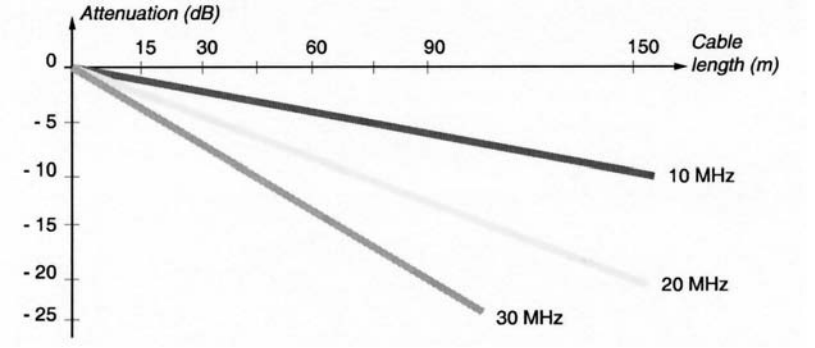

Figure 8.13 PLC signal attenuation according to inside cable length

Table 8.8 Distance for PLC Signal Propagation over External Cables

PLC TECHNOLOGY	*CABLE TYPE*	*DISTANCE*	*TCP BIT RATE (MBIT/S)*
Oxance HomePlug Turbo (1.1)	Buried	1,300m	3
Spidcom	Buried	3,000m	3

are therefore relatively insensitive to electromagnetic disturbances, or aerial cables, in which case they are more sensitive to electromagnetic disturbances but much less so than inside cables that are subject to disturbances close to those of various domestic devices.

Table 8.8 summarizes the results obtained for various PLC technologies.

Interference

The interference notion is essential in PLC networks. The PLC signal that propagates over electrical wirings causes electromagnetic emissions in the 1 to 30 MHz frequency band in the cables' immediate environment and is itself disturbed by the electrical devices connected to the electrical network.

In addition, a link between two PLC stations does not necessarily have the same characteristics in both communication directions. The physical characteristics of the communication medium (impedance, charge, capacity) can therefore change according to the signal propagation direction.

The various national, European, and international standardization bodies have set up regulations intended to determine the electromagnetic emissions limits for PLC devices operating over an electrical network. As we saw in Chapter 1, the electromagnetic emissions of these devices must remain less than a set maximum quasipeak value. This PSD (power spectral density) boundary value has been defined by the IEC CISPR 22 amendment as being –50 dBm/Hz.

Effects of Interference on the Electrical Network

The PLC network is subject to interference and electromagnetic disturbances originating from the electrical devices connected to the network outlets.

Figure 8.14 illustrates the disturbance sources that a PLC local area network can receive.

The use of electrical devices and their actuation generate various noises (broadband, impulse, Gaussian, and so forth) that can be evaluated to an average noise of amplitude 30 dBìV/m over the entire 1- to 30-MHz frequency band.

It is difficult to make an exhaustive list of devices generating these noises, but many devices have been identified as potential sources: plasma displays, halogen lamps, vacuum cleaners, light regulators, microwave ovens, television sets, computer screens, air conditioning, heating appliances, and so forth.

Figure 8.15 illustrates the various disturbances of electrical devices as a mean value of various measurements performed on many domestic installations according to the day hours. The end of the day is obviously loaded with disturbances since many devices simultaneously operate on the electrical network. In the figure, we see that the disturbance amplitude varies according to the frequency, with two higher amplitude peaks being around 10 MHz and 20 MHz.

The technologies have greatly improved to ensure the robustness of data communications over electrical wirings, but it may be necessary to take some precautions with some electrical devices like halogen lamps or vacuum cleaners connected to the same outlet as a PLC device.

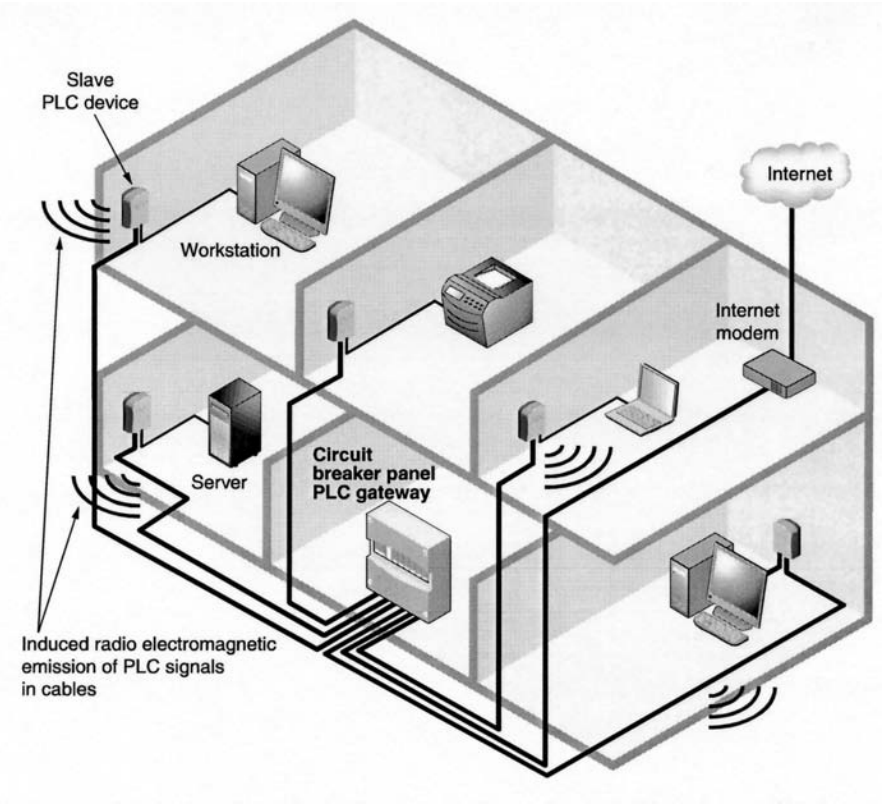

Figure 8.14 Electromagnetic disturbances caused by PLC devices connected to the electrical network

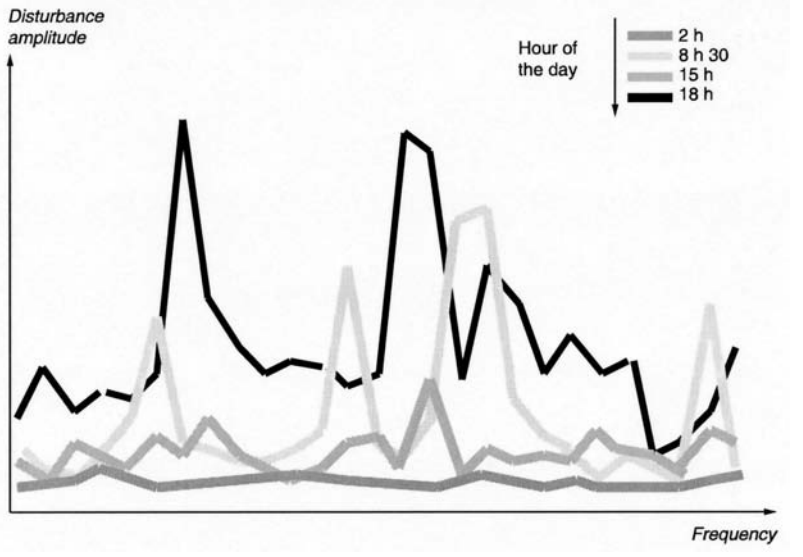

Figure 8.15 Disturbance amplitude on a domestic electrical network according to the hours of the day

Figure 8.16 illustrates how a power strip must be used with a PLC device. A power strip is inherently a source of noise for PLC devices to which the noise of disturbing devices connected to it must be added. In all cases, it is preferable to connect the PLC device directly to the wall outlet whenever possible or to connect it to a "biplite" (two outlet wall power strip).

Network Data Rates

In addition to electromagnetic disturbances, a PLC network is subject to constraints related to the technology itself. These constraints relate to the data rate that never corresponds to the expected rate and security.

The theoretical data rate of HomePlug 1.0 networks is between 1 Mbit/s and 14 Mbit/s. The 14-Mbit/s data rate is only a theoretical value roughly corresponding to a useful throughput of 5 Mbit/s, i.e., 0.625 Mb/s. HomePlug Turbo and AV provide a theoretical data rate of 5 to 85 Mbit/s and 10 to 200 Mbit/s, respectively, for a useful throughput of 1 to 20 Mbit/s and 5 to 60 Mbit/s, respectively.

The size of the frame headers used in HomePlug and the use of a number of mechanisms enabling a reliable transmission in an electrical environment mainly explain this difference. Part of the transmitted data is used for the control and management of the transmission to make it reliable. Only a fraction of the data rate emitted by the device corresponds to the conveyance of the data itself.

Useful Throughput Calculation

The useful throughput corresponds to the rate for data transmitted at OSI layer level *n*. The useful throughputs of levels 1, 2, 3, and so forth correspond to the rates

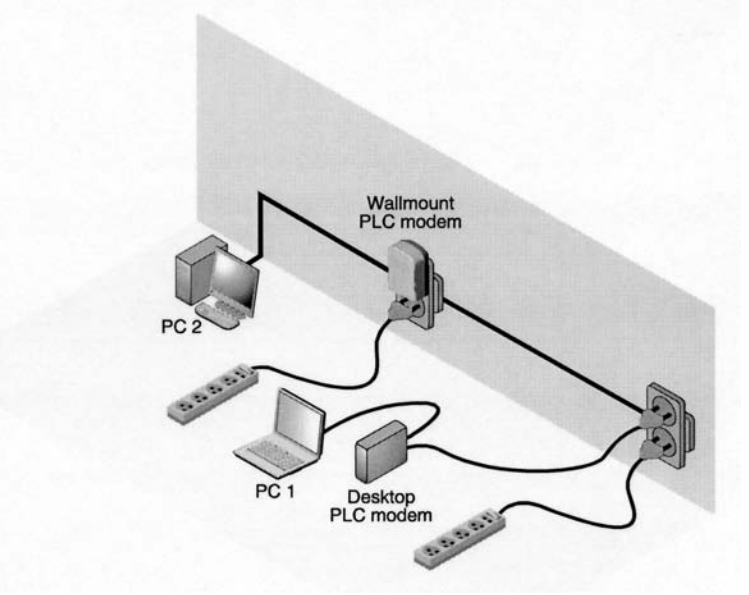

Figure 8.16 Optimum use of power strips and double outlets

for data at these levels, which is calculated according to the overhead used for managing and sending the transmission.

As we saw in Chapter 5, the data sent over this electrical interface corresponds to a physical frame, or PLCP-PDU. This frame consists of a PLCP header comprised of two fields and data originating from the MAC layer. As illustrated in Figure 8.17, each part of the PLCP-PDU is sent at different speeds.

The PCLP-PDU header includes start and end delimiters. These headers are transmitted at a speed of 1 Mbit/s in the case of the long preamble.

The second PLCP-PDU field corresponds to the MAC frame itself. This frame is sent at rates that can be as high as 1 to 4.5, 9, or 14 Mbit/s as far as HomePlug 1.0 is concerned. The PLC uses its data rate variation mechanism to transmit at different rates according to the characteristics of the electrical environment.

The transfer time, which is equal to the propagation time increased by the transmission time, must be known to calculate the level 2 useful throughput. Since the electrical interface is used as the transmission medium, we can consider that the propagation time is equal to zero, as the electron moving speed over an electrical wiring is equivalent to the speed of light. The transmission time (Tt) therefore corresponds to the time required for data sending.

By definition, the level 2 useful throughput (Du) corresponds to the volume of transmitted payload divided by the overall transmission time, i.e.:

$$Du = \frac{Data}{Tt}$$

Let us consider a HomePlug 1.0 network whose frames use a short preamble and in which the transmission speed is 14 Mbit/s for all the stations. We are going to calculate the useful throughput (Du_1) of a PLCP-PDU when sending 1,500-byte data. Since the payload size is known, the transmission time, which is equivalent to the sum of the PLCP-PDU header transmission time and of the MAC data transmission time, is still to be calculated.

The MAC frame data comprise a 34-byte header. Therefore, their size is 1,534 bytes. Their transmission time (Tt_{MAC}) is given by the following formula:

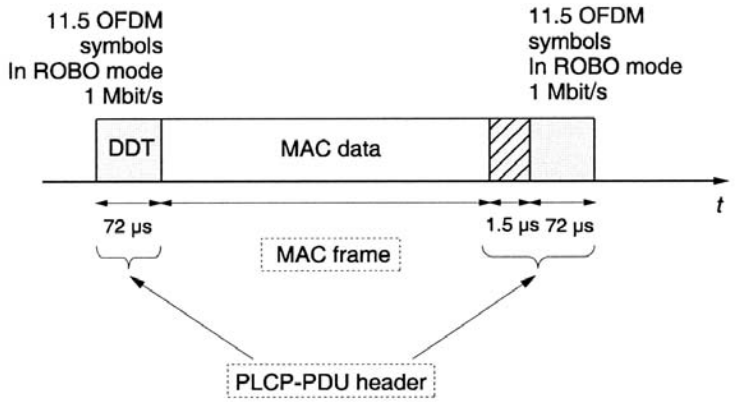

Figure 8.17 Structure of a PLCP-PDU

$$Tt_{\text{MAC}} = \frac{1{,}534 \text{ bytes} \times 8 \text{ bit/byte}}{14 \text{ Mbit/s}} \approx 0.000876\text{s}$$

The 120-bit PLCP-PDU header is sent at a rate of 1 Mbit/s. Therefore, its transmission time ($Tt_{\text{PLCP-PDU}}$) is:

$$Tt_{\text{PLCP-PDU}} = 72\ \mu s + 1.5\ \mu s + 72\ \mu s \approx 145.5\ \mu s$$

The total transmission time (Tt_1) is therefore equivalent to:

$$Tt_1 = Tt_{\text{MAC}} + Tt_{\text{PLCP-PDU}} \approx 0.0010215\text{s}$$

The useful throughput is equivalent to the volume of transmitted information, i.e., 1,500 bytes (12,000 bits) divided by the transmission time, i.e., 1.021 ms, which corresponds to 11.74 Mbits/s:

$$Du_1 = \frac{1{,}500 \text{ bytes} \times 8 \text{ bit/byte}}{Tt_1} \approx 11.74 \text{ Mbit / s}$$

However, this data rate does not correspond to the reality. In the PLC, the sending of data must comply with some rules related to the CSMA/CA (carrier sense multiple access/collision avoidance) access method. This method is based on certain mechanisms detailed in Chapter 3 that generate a rather high overhead.

In the ideal case where a single station transmits over the medium, when the station transmits data, it listens to the medium. If the medium is free, it defers its transmission while it waits for a CIFS time. When the CIFS times out, and if the medium is still free, it transmits its data. Once the data transmission is completed, the station waits for an RIFS time to know whether its data have been acknowledged. As illustrated in Figure 8.18, the minimum overhead generated by the transmissions of the CIFS and RIFS timers of the ACK and of the headers is far from being negligible.

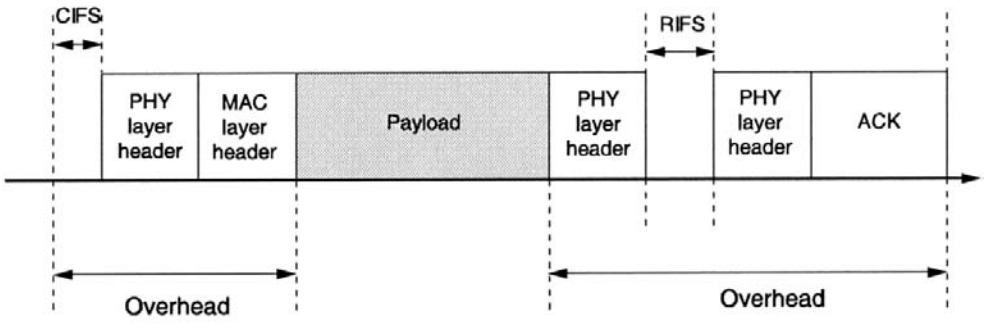

Figure 8.18 Minimum overhead when transmitting data

We are going to calculate the useful throughput associated with this ideal case (Du_2). As in the example above, we consider the use of short preambles for 1,500-byte data transmitted at a speed of 14 Mbit/s.

According to our preceding calculations, the data transmission time corresponds to Tt_1, i.e.:

$$Tt_{\text{Data}} = \frac{1{,}534 \text{ bytes} \times 8 \text{ bit/byte}}{14 \text{ Mbit/s}} + 145.5\mu s \approx 0.001670\text{s}$$

Since the duration of the ACK frame is 72 μs, its transmission time is equal to:

$$Tt_{\text{ACK}} = 72\mu s + 145.5\mu s = 0.0002175\mu s$$

CIFS and RIFS are fixed value timers. However, this value varies from one technology to another. For HomePlug 1.0, the value is 35.84 μs for CIFS and 26 µs for RIFS.

Therefore, the overall transmission time is equal to:

$$Tt_2 = \text{CIFS} + Tt_{\text{Data}} + \text{RIFS} + Tt_{\text{ACK}} \approx 0.001949\text{s}$$

In our ideal case, the useful throughput is therefore equal to:

$$Du_2 = \frac{1{,}500 \text{ bytes} \times 8 \text{ bit/byte}}{Tt_2} \approx 6.157 \text{ Mbit/s}$$

We notice that the higher the overhead, the lower the useful throughput. Since a single station transmits over the medium, this data rate corresponds to the maximum useful throughput.

Everything gets more complicated when the network consists of more than two stations that simultaneously attempt transmissions over the medium. When a station hears that the medium is busy after trying to get access to the medium or after waiting for a CIFS, it defers its transmission. For this purpose, it triggers a timer calculated using the back-off algorithm.

The additional waiting time and the random back-off timer obviously increase the overhead as illustrated by Figure 8.19.

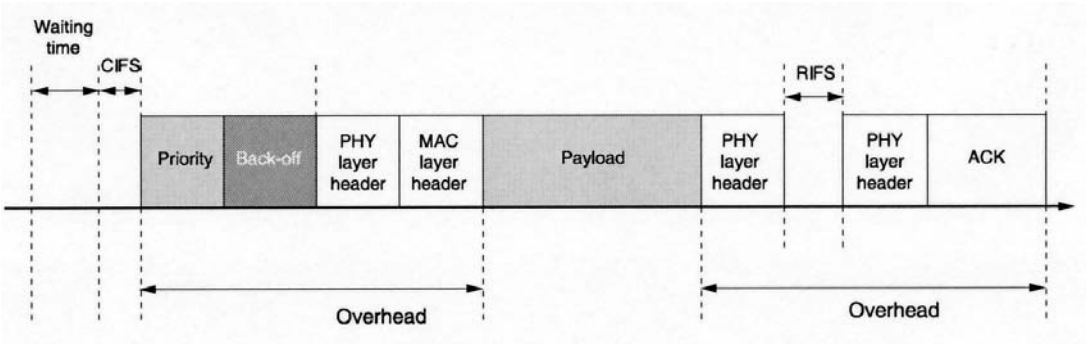

Figure 8.19 Maximal overhead when transmitting data

The transmission time (Tt3) becomes:

$$Tt_3 + T_{\text{Wait}} + \text{CIFS} + T_{\text{Backoff}} + Tt_{\text{Data}} + \text{RIFS} + Tt_{\text{ACK}}$$

Since the waiting time and the back-off timer are not fixed, it is difficult to determine their values. However, we can consider that the sum of the waiting time and back-off time is generally equivalent to the transmission time in the ideal case. The back-off timer can be considered as zero compared with the waiting time. As for the waiting time, it corresponds to the transmission time of another station.

Therefore, the useful throughput is equivalent to:

$$Du_3 = \frac{\text{Data}}{Tt_3} = \frac{\text{Data}}{T_{\text{Wait}} + T_{\text{Backoff}} + Tt_1}$$

and is formulated as:

$$Du_3 \approx \frac{\text{Data}}{2Tt_1} \approx \frac{Du_2}{2}$$

When the network consists of two stations, the useful throughput of each station is almost equal to the maximum useful throughput divided by the number of stations forming the network. This formula can be generalized for a PLC network consisting of *n* stations transmitting at the same speed.

The useful throughput for each station is equivalent to:

$$Du_3 \approx \frac{Du_2}{n}$$

In addition, only the level 2 useful throughput was taken into account in our preceding calculations. However, the MAC frame data correspond to an LLC frame with a 4-byte header containing an IP packet with a 20-byte header. The IP packet itself includes a TCP segment with a 24-byte header containing user data. Therefore, we have a total of 48 additional overhead bytes. Data processing for the upper layers (layers 3 and 4), which also generates overhead, was not taken into account.

To conclude, we can say that a PLC network never reaches the claimed capacity on the physical medium. If data is transmitted at the speed of 14 Mbit/s, the number of data bits for the user only represents approximately half of the raw capacity of the electrical interface, i.e., 5 Mbit/s (625 Kb/s) in our example on average.

Table 8.9 summarizes the useful throughputs of various types of local area networks.

Compared with the transmission speed over the medium, the useful throughput is much higher in Ethernet than in PLC.

Maximum PLC Actual Data Rate

After calculating PLC level 2 useful throughputs in the preceding section, we'll go to an upper level. For this purpose, we'll use the Iperf traffic generator available at the following address: http://dast.nlanr.net/Projects/Iperf/.

Table 8.9 Useful Throughputs of Local Area Networks

NETWORK	*THEORETICAL DATA RATE (Mbit/s)*	*USEFUL THROUGHPUT (Mbit/s)*
Ethernet 10	10	8.08
Ethernet 100	100	90.06
HomePlug 1.0	14	5.1
HomePlug Turbo	85	40
HomePlug AV	200	150

Iperf is used for generating any type of traffic between a client and a server. For our test, illustrated in Figure 8.20, we use the following components:

- An IBM R50e computer running under Windows XP SP2;
- A DELL Latitude D600 computer running under FreeBSD 5.4;
- Two PLC modems complying with the same technology (HomePlug 1.0, Turbo, AV, and Spidcom 200) for each computer;
- Two category 5 shielded FTP Ethernet cables;
- A standard four-outlet power strip.

The client (192.168.1.100), the server (192.168.1.110), and the access point (192.168.1.120) must be configured so as to have the same network address; failing this, no communication can take place.

The test consists of generating a 100-Mb TCP traffic and in verifying the associated useful throughput according to the crossed network or to the mechanisms used. Each value corresponds to the mean of three tests to ensure reliability by excluding too high an oscillation.

In the server, all you have to do is to enter iperf –s in a MS-DOS window to initiate the server. On the client side, the TCP transmission of 100 Mb is initiated by entering iperf –c 192.168.1.110 –n 100000000 in a MS-DOS window.

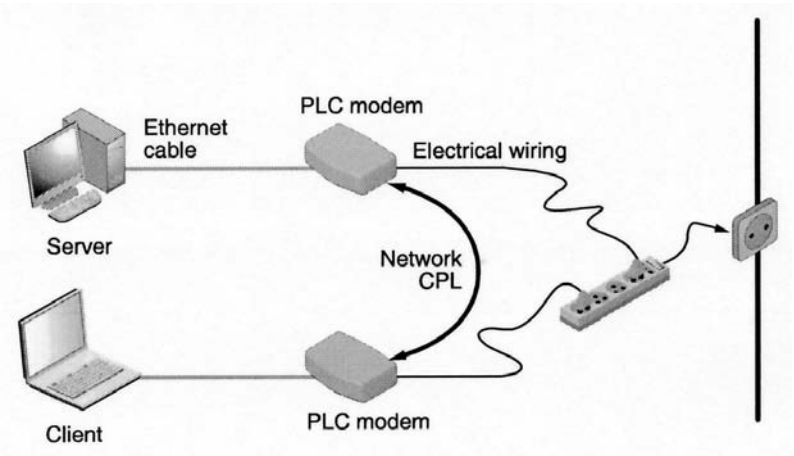

Figure 8.20 Test configuration

Table 8.10 shows the results obtained for various technologies with this test bed.

Table 8.11 summarizes the necessary data rates for certain usual Internet applications (data, voice, or video applications).

Data Rate Variation

In a PLC network, the constraints related to the electrical interface can result in a variation of the data rate provided by the network. As previously explained, interference originating from the electrical devices and the multiplication of PLC devices on the electrical network are some examples that can cause data rate variations.

The PLC data rate varies automatically as soon as interference occurs in the environment. This is a user-transparent mechanism. So, the HomePlug 1.0 data rate changes from 14.1 Mbit/s to 12.83, 10.16, 8.36, 6.35, 4.04, 2.67, and even to 0.9 Mbit/s when the environment is highly degraded.

A different data rate can be given to any of the network's stations with the automatic data rate variation scheme.

Figure 8.21 illustrates the variation of the theoretical data rate and of the useful throughput following measurements performed during tests with the Iperf tool.

When the network is comprised of several stations, we have seen that the data rate for each station corresponds to the maximum useful throughput divided by the number of stations. However, we have considered that the waiting time is equal to the transmission time for a given station considering that the transmission speed is equal for all stations.

Table 8.10 Maximum Actual Data Rates of PLC Technologies

STANDARD OR TECHNOLOGY	*USEFUL THROUGHPUT (Mbit/s)*	*MAX. ACTUAL DATA RATE (Mbit/s)*
HomePlug 1.0 (14 Mbit/s)	5.1	4.35 Mbit/s
HomePlug Turbo (85 Mbit/s)	40	11.5 Mbit/s
HomePlug AV (200 Mbit/s)	150	60.5 Mbit/s
DS2 (200 Mbit/s)	150	61.2 Mbit/s

Table 8.11 Necessary Data Rates for Typical Internet Applications

APPLICATION	*NECESSARY BIT RATE*
Surf over Internet and e-mail: –down –up	 50 Kbit/s 5 Kbit/s
Voice over IP	80 Kbit/s
Streaming audio: –down –up	 80 Kbit/s 14 Kbit/s
SDTV video channel	1.5 Mbit/s
HDTV video channel	8 Mbit/s

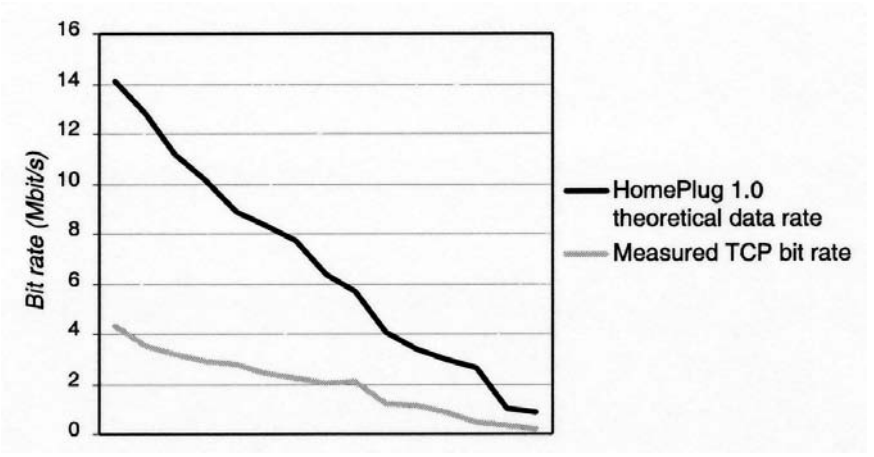

Figure 8.21 Theoretical data rate and useful throughput variation with the HomePlug 1.0 technology

In the case of all the stations' different speeds, the waiting time is prolonged. Because of this, the global network data rate falls heavily. If a station of the network transmits at a speed of 1 Mbit/s, its transmission time is 14 times higher than that of a station transmitting at 14 Mbit/s. Therefore, this station must wait 14 times longer before transmitting its data. Its average useful throughput tends to be around 1 Mbit/s.

Figure 8.22 illustrates the likelihood of data collision over the electrical network according to the number of connected live PLC devices.

Security

Unlike Wi-Fi networks, PLC networks provide top class security insofar as the medium cannot be accessed (electrical wirings buried in the walls or in packages) and is also not dangerous.

Therefore, security is achieved from the moment the user implements a satisfactory password configuration on its PLC network. We detail this configuration in the following chapters dedicated to the implementation of a PLC local area network.

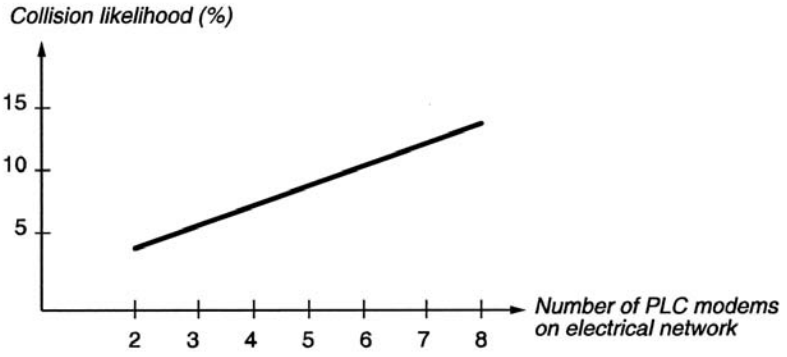

Figure 8.22 Likelihood of collisions according to the number of PLC modems on the electrical network

CHAPTER 9

Configuration

The installation of a PLC network is rather simple. All you have to do is connect the PLC devices to an Ethernet network or to a modem (ADSL, cable, STN, and so forth) while taking into account the constraints mentioned in the previous chapter.

The configuration of the network PLC devices and the terminal interfaces (generally PC network interface cards) connected to PLC devices follows the network installation. The configuration of the PLC devices and of the Ethernet boards of the connected terminals are detailed in this chapter. The various functionalities provided by these devices according to the targeted use (domestic, professional, or industrial) are also detailed.

The configuration of the terminal (PC) concerns the installation and the software configuration of the network interface card, whether this is an external, Ethernet or USB card. The board installation differs depending on the operating system used. Its configuration is almost similar from one system to another since it is based on the parameters of the PLC technology used (HomePlug, DS2, and so forth).

The following sections describe the parameters to be configured according to the main existing PLC technologies, even though the HomePlug specification is now the de facto PLC standard, considering its prevalence on the PLC device market.

Once the network interface card is configured, the terminal is still not quite ready to communicate with the network. It is still necessary to assign suitable network parameters, such as IP address, mask, and so forth to it in order to set up communication.

Configuring a HomePlug 1.0 or Turbo Network

Configuring a PLC network with HomePlug version 1.0 Turbo devices is relatively simple, insofar as all the network devices have the same hierarchical function with the network in peer-to-peer mode. For HomePlug AV devices, the network mode used is a mode in which one of the devices is the central coordinator (CCo) and the other is stations (STA). However, this is transparent to the end user who configures all the HomePlug AV devices on the electrical network in the same way.

Devices on the market based on the HomePlug specification are configured in the same manner and are compatible between themselves. Various tools are used for

configuring them according to the targeted operating systems. They are described for Windows XP as well as for the Linux and FreeBSD systems.

Configuring a PLC Network Under Windows

Almost all the tools used for configuring HomePlug PLC devices have the same functionalities for the configuration of HomePlug chip parameters. As we have seen in Chapter 7, HomePlug chips mainly originate from the Intellon manufacturer. They are used for reading a number of values stored on the quality of exchanges between PLC devices. The PLC network is configured and optimized using these values.

Among the HomePlug parameters that can be configured, let's mention the following ones in particular:

- The NEK (network encryption key) used for securing data exchanges in the same PLC local area network;
- The DEK (default encryption key) used for configuring the NEK on all the remote PLC devices scattered over the electrical network;
- The PLC device transmission priority among four possible ones (CA0, CA1, CA2, CA3) used for configuring some PLC devices like gateways to other networks, in particular Ethernet.

Table 9.1 summarizes the main parameters which can be read and presented to the PLC network user with HomePlug configuration tools.

Estimating the PHY Data Rate of Communications Between PLC Devices

The various PLC devices store the instantaneous value of the "bytes in 40 symbols" parameters exchanged by the devices in the HomePlug chip. This value is used for estimating the PHY data rate (at the physical layer level) between PLC devices, as we have seen in Chapter 3.

The maximum PHY data rate corresponds to the number of data (or bits) ensuring the best possible modulation coded with 40-symbol OFDM blocks of duration 8.4 μs.

This gives, for HomePlug 1.0 and Turbo:

HomePlug 1.0:

$$Datarate_{PHMAXY} = \frac{519 \times 8}{40 \times 8.4} = 12{,}35714286 \text{ Mbit/s}$$

HomePlug Turbo:

$$Datarate_{PHMAX} = \frac{2{,}812 \times 8}{40 \times 8.4} = 66{,}95238095 \text{ Mbit/s}$$

Still using the data mentioned in Chapter 3, the PHY data rate can be calculated according to the values given by the HomePlug chip:

HomePlug 1.0:

$$Datarate_{PHY} = \frac{588 - 38}{481} \times \frac{BYTES_{in\,40symbols}}{42} + \left(14 - \frac{588 - 38}{481} \times \frac{519}{42}\right) \text{Mbit/s}$$

Table 9.1 HomePlug Parameters Visible by Configuration Tools

HomePlug PARAMETER	*INDICATIONS*
Bytes per 40 symbols	Number of bytes per block with 40 OFDM symbols (used for calculating the estimated PHY data rate for HomePlug 1.0)
Bytes per 336 us Block (for HomePlug Turbo)	Number of bytes per 336-is block (used for calculating the estimated PHY data rate for HomePlug 1.1 Turbo, sometimes called Viper)
DATA_TX_COUNT	Transmitted data number counter
FAILS Received	Number of received FAIL type frames
Frame Drops	Number of lost frames
ACK Counter	Number of sent ACK type frames
NACK Counter	Number of sent NACK type frames
FAIL Counter	Number of sent FAIL type frames
Contention Loss Counter	Number of lost contention frames
CA0 Latency Counter	Total number of milliseconds between receipt of a CA0 frame sending request and successful access to transmission channel
CA1 Latency Counter	Total number of milliseconds between receipt of a CA1 frame sending request and successful access to transmission channel
CA2 Latency Counter	Total number of milliseconds between receipt of a CA2 frame sending request and successful access to transmission channel
CA3 Latency Counter	Total number of milliseconds between receipt of a CA3 frame sending request and successful access to transmission channel
Cumul Bytes per 40 Symbols Packet Counter	Cumulated received frames in number of 40 OFDM symbols
MAC Address	MAC addresses of other PLC devices on the same network

HomePlug Turbo:

$$Datarate_{PHY} = \frac{BYTES_{per\,336\,\mu sblock} \times 8}{40 \times 8.4}\ \text{Mbit/s}$$

where $Bytes_{per336\mu sblock}$ represents the number of bytes in a data block at the physical layer level of duration 336 μs.

As we have seen in Chapter 8, there is a difference between the physical data rate and the useful throughput for the user. Table 9.2 gives an estimated correspondence between these two data rates since HomePlug PLC configuration tools only indicate the physical data rate for the user.

Among the various HomePlug 1.0 and Turbo PLC configuration tools, let's mention the following tools that differ in their interfaces and user friendliness:

- *MicroLink dLAN from MicroLink Informer from Devolo AG*. The first one is used for configuring the PLC network and the second one for checking the network status.
- *PowerPacket Utility from Intellon*. This enables the same parameterizations as the Devolo tool using various tabs for the various configuration operations (NEK of the PLC logical network illustrated by Figure 9.1, main tab for man-

Table 9.2 Correspondence Between Indicated Physical Data Rate and Useful Throughput

	PHYSICAL BIT RATE (Mbit/s)	*USEFUL THROUGHPUT (Mbit/s)*
HomePlug 1.0	14	4.5 to 5
	12.83	3.5
	11	3.2
	10.16	2.9
	8.36	2.4
	6.35	2
	4.04	1.22
	3	0.89
	1	0.33
	0.9 (ROBO mode)	0.2
HomePlug Turbo	85	12.5
	75	11.8
	55	9.42
	45	8.79
	35	8.23
	25	7
	14	4.5
	12.83	3.5

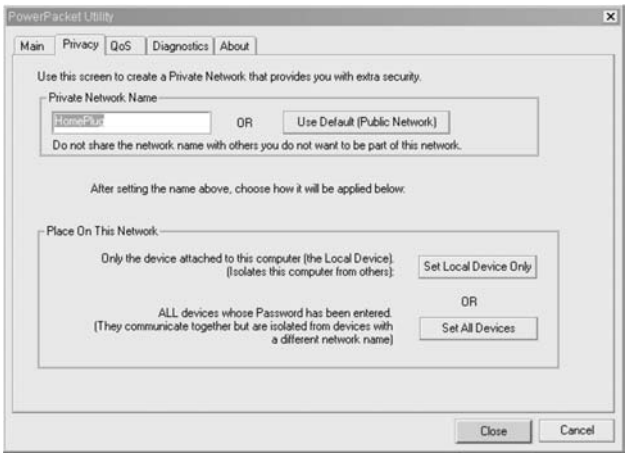
PowerPacket Utility
Main
Privacy
QoS
Diagnostics
About
Use this screen to create a Private Network that provides you with extra security.
Private Network Name
OR
Use Default (Public Network)
Do not share the network name with others you do not want to be part of this network.
After setting the name above, choose how it will be applied below:
Place On This Network
Only the device attached to this computer (the Local Device).
(Isolates this computer from others):
Set Local Device Only
OR
ALL devices whose Password has been entered.
(They communicate together but are isolated from devices with a different network name)
Set All Devices
Close
Cancel

Figure 9.1 Encryption key configuration for HomePlug devices

agement of the PLC network, Figure 9.2, management of priority levels for each VLAN illustrated by Figure 9.3).

- *SoftPlug from LEA-Thesys* (http://209.236.239.167/Images/Upload/support_telechargement/SetupSoftPlug.msi).

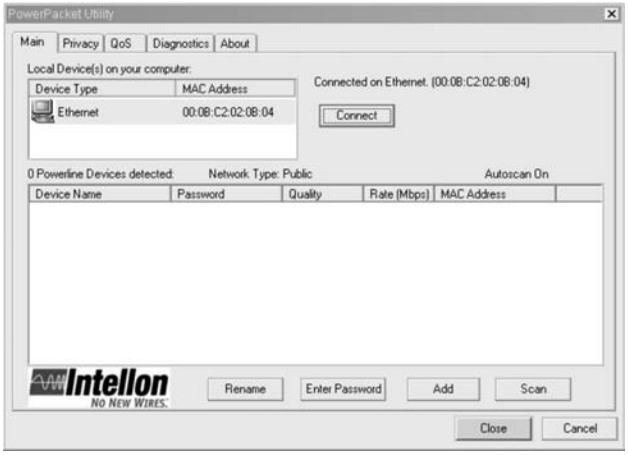

Figure 9.2 PowerPacket configuration utility from Intellon in main tab

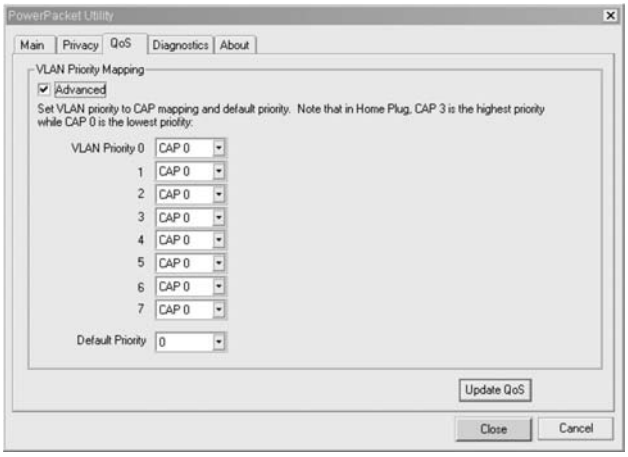

Figure 9.3 Configuration of priority levels for each VLAN in HomePlug

This tool provides the same functionalities as the previous tools but with an interface which is perhaps easier to use.

Most PLC modems have Ethernet interfaces. However, some of them provide USB interfaces used for emulating a "virtual" Ethernet interface which will be viewed as a new network interface by the connecting terminal.

Since the behavior of virtual network interfaces on the USB interface proves to be unstable, it is recommended to equip PLC devices with an Ethernet interface and an RJ-45 connector.

Configuring an Ethernet or USB PLC Device

For this example relating to the configuration of a PLC device, we have selected the Intellon Power Packet Utility configuration tool.

Once the tool is downloaded, we can proceed with the installation. Once the installation is completed, the Power Packet Utility program can be started (via Start, Programs). The program proposes several tabs corresponding to the various available functionalities as illustrated by Figure 9.4.

To build a secure PLC local area network, it is necessary to start with the configuration of the NEK for the various devices to be connected to the network.

In the Security tab, start with the entry of a 4-to-24-character name in the Private network name field. This name is equivalent to the password of the NEK common to all PLC network devices. The default value is HomePlug.

Any PLC device complying with the HomePlug standard bought in stores can be connected to a PLC network for which the NEK password default value was kept. Insofar as the signal propagates beyond the electrical meter of the house, anybody can connect to this private local area network. This is why it is very important for PLC network security purposes to change this default value. Figure 9.5 shows the default password.

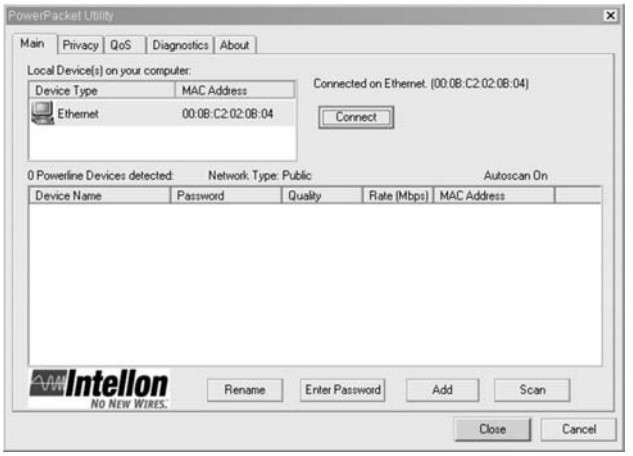

Figure 9.4 Products tab of PLC configuration tool

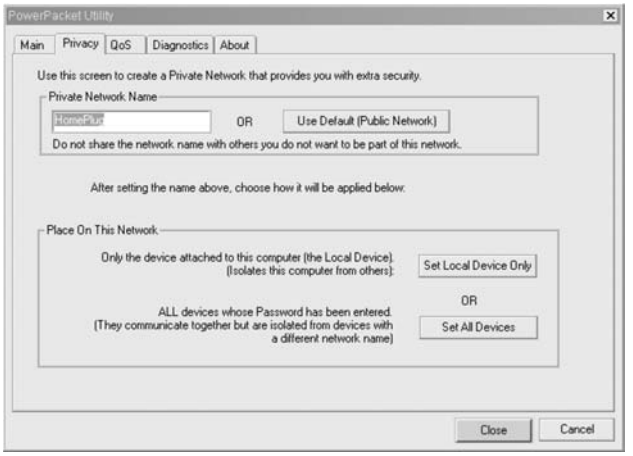
PowerPacket Utility
Main
Privacy
QoS
Diagnostics
About
Use this screen to create a Private Network that provides you with extra security.
Private Network Name
HomePlug
OR
Use Default (Public Network)
Do not share the network name with others you do not want to be part of this network.
After setting the name above, choose how it will be applied below:
Place On This Network
Only the device attached to this computer (the Local Device).
(Isolates this computer from others):
Set Local Device Only
OR
ALL devices whose Password has been entered.
(They communicate together but are isolated from devices with a different network name)
Set All Devices
Close
Cancel

Figure 9.5 Security tab of PLC configuration tool

In Figure 9.6, the NEK password has been replaced with the PLC Network value. The longer this password is, and the more numbers and symbols it has, the harder it is to crack for an intruder looking to access the PLC network.

All the PLC devices connected to the electrical network can be configured from this configuration interface, whether these already exist in the PLC local area network or not. All you have to do is know the DEK of the remote devices connected to the electrical network.

The DEK is unique for each PLC device and its ID is indicated at the back of the device. It can be called SecureID (Devolo), Password (Corinex and Oxance), Mot de passe (LEA), and so forth. This key is encoded in 16 bytes in the hexadecimal format.

In Figure 9.7, the value of the DEK is JJMZ-QFDI-RVHE-OJRS above the MAC address of the PLC device to be configured. The DEK is secured.

If you know the value of the DEK, just click on the Add Products tab and enter this value in the Password field. The Adapter name field is used in order to identify the PLC device (living room or bedroom, for example).

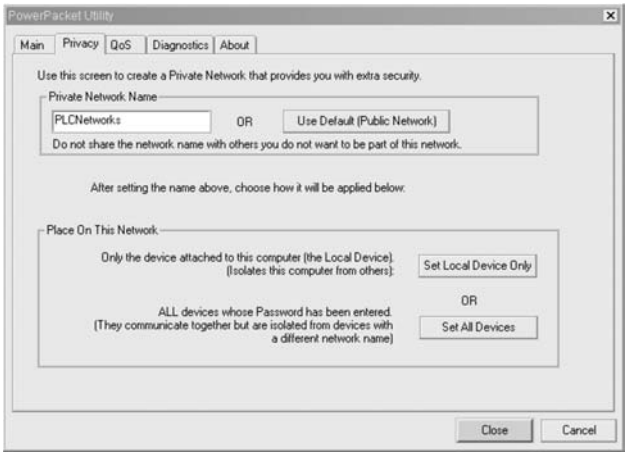
PowerPacket Utility
Main
Privacy
QoS
Diagnostics
About
Use this screen to create a Private Network that provides you with extra security.
Private Network Name
PLCNetworks
OR
Use Default (Public Network)
Do not share the network name with others you do not want to be part of this network.
After setting the name above, choose how it will be applied below.
Place On This Network
Only the device attached to this computer (the Local Device).
(Isolates this computer from others):
Set Local Device Only
OR
ALL devices whose Password has been entered.
(They communicate together but are isolated from devices with a different network name)
Set All Devices
Close
Cancel

Figure 9.6 PLC local area network password configuration

Figure 9.7 Reading the DEK key on the box of a PLC device

Figure 9.8 illustrates the configuration of a PLC local area network using DEK read on the living room and bedroom devices connected to the same electrical network.

Once all the network PLC devices are configured locally or using the DEK key, simply select the Products tab to check the status of the PLC links between the device to which the PC is connected and other PLC devices connected to the electrical network (see Figure 9.9):

- The "Product(s) connected to your PC" window indicates the PLC device or devices with direct Ethernet connection to the configuration PC via the PC network interface card and its MAC address.
- The "Product(s) sensed" window lists the PLC devices sensed on the electrical network that have the same NEK and indicates their estimated data rate.

The products in the list can be renamed by clicking on rename and indicating a relevant name to retrieve the PLC device in the electrical network architecture. The PLC devices were renamed living room and bedroom in Figure 9.9.

Coexistence of Several HomePlug PLC Local Area Networks on the Same Electrical Network

Several NEK cannot be configured on the same HomePlug 1.0 and Turbo PLC device. Therefore, a device cannot belong to several PLC local area networks. Within the framework of the HomePlug AV specification, it will be possible to have several encryption keys on the same PLC device and therefore to have devices belonging to several PLC local area

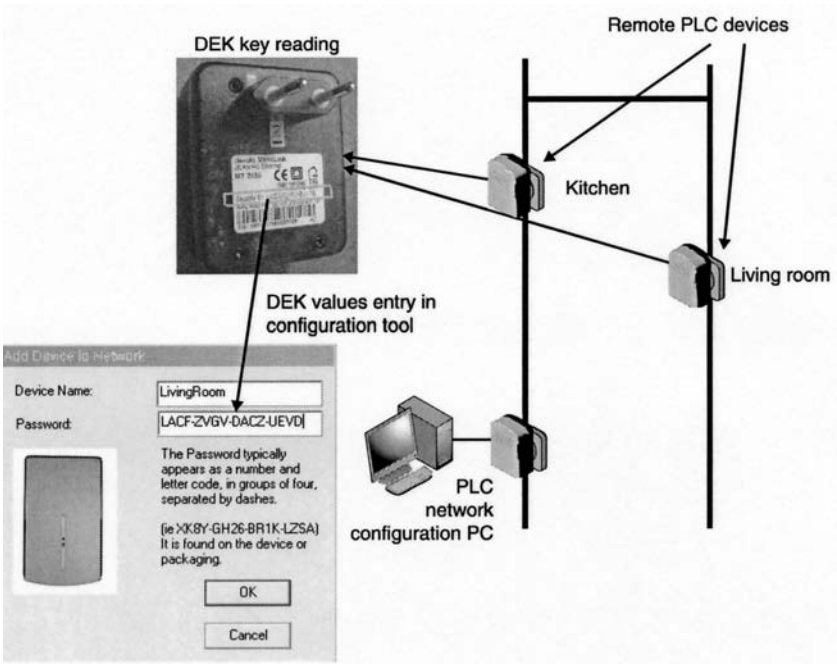

Figure 9.8 PLC network configuration using the DEK

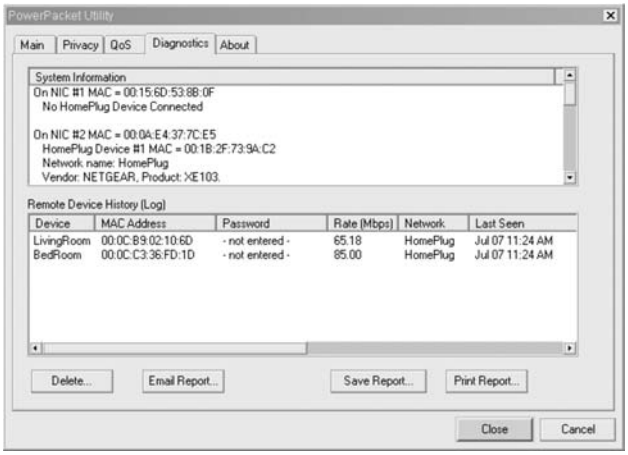

Figure 9.9 PLC network status diagnostic function

networks. It is possible to have several PLC local area networks on the same electrical network. These PLC local area networks just have to share the frequency band (from 1 to 30 MHz) and divide their transmission speed by the number of existing PLC local area networks.

Since the PLC network configuration is now completed, the IP network and the suitable applications can be configured for the users of the Ethernet network consisting of the PLC network. This IP network configuration is detailed in Chapter 10.

By clicking on the "Diagnostics" tab, system information can be displayed on the PC and PLC device directly connected to the PC using Ethernet as well as histories on PLC products previously sensed by the configuration tool.

Figure 9.9 illustrates this tab for the bedroom device corresponding to the PLC network (PLCNetworks) with the date and time of the last display of this device. Just click on "Print" to save or send these histories to other PLC network installers.

Configuring a HomePlug AV Network

Concerning the HomePlug AV standard, there are several standard implementations based on specifications with two chips manufactured by Intellon with the integrated 1.0 and 1.1 firmware versions.

Table 9.3 indicates the functionality differences between the versions based on the INT6000 and INT6300 Intellon chips.

For easier configuration of a PLC network for end users able to broadcast PLC technologies by ISP in order to broadcast HDTV flows from IPTV offers in a home environment, there are two PLC network configuration modes:

- Configuration using an embedded user interface on a PC or a gateway for Internet access (in general, via the Web interface of this gateway).
- Configuration using the EasyConnect mode used for easily implementing a HomePlug AV PLC network. This mode consists of using the connection buttons installed on HomePlug AV PLC devices fitted with the INT6300 chip. To configure a new network, the button of the first device must first be depressed

Table 9.3 Various Chip and Firmware Versions for HomePlug AV Standard

Functionalities	*1.0*	*1.1*	*Advantages*
Chips	*INT6000*	*INT6300*	
Firmware	*1.x*	*3.x*	
128-bit encryption	Yes	Yes	Provides security to the powerline network
CSMA/CA Channel access	Yes	Yes	Provides reliable network connection
CCO Failover	Yes	Yes	Controls redundancy of powerline connection
QoS (VLAN, TOS)	Yes	Yes	Provides better user experience on video streaming, VoIP, online gaming
Rotate NEK encryption	Yes	Yes	Provides a highly secured powerline network
IGMP v3	No	Yes	Provides an efficient network connection
Signal Strength LED	No	Yes	Serves as an excellent tool for powerline network site survey
One button encryption	No	Yes	User-friendly encryption set up
Factory default reset	No	Yes	Provides user-friendly reset when deploying the network in house

for 2 seconds. The power on indicator light of the package then blinks. The user then has 1 minute to depress the EasyConnect buttons of the other devices he wants to include into his logical PLC network. The buttons of the other devices must also be depressed for 2 seconds to associate them with the first device. Once the devices are associated, the PLC activity lights are fixed on the various network stations; the PLC network is then configured. Figure 9.10 illustrates the principle for associating new stations with the PLC network using the EasyConnect mode.

Concerning the tools for configuring a HomePlug AV PLC network, several are available for managing the notions of encryption keys and priorities of the various devices with various user interfaces depending on the manufacturers. Some of these are mentioned below:

- *AZtech HomePlug AV Utility* (downloadable at the following address: ftp://ftp.aztech.com/support/malayia/HomePlug/HL108E%20HomeplugAV%20Utility%20v1.0.zip)
- *Zyxel PLA PLA tool* (downloadable at the following address: http://us.zyxel.com/upload/download_library/PLA-470_3.0.5(AP).zip)
- *Devolo dLAN Software* (downloadable at the following address: http://download.devolo.net/webcms/015587800119090894/dlan-software-v17.exe)
- Linksys PLE 200 Utility (downloadable at the following address: ftp://ftp.linksys.com/downloads/NA/firmare/PLE200%20FW3.3%20Rev2%20NA.zip)
- *AsokaUSA PowerManager* (downloadable at the following address: http://asokausa.com/downloads/PowerManager1.2.0-Common.zip)

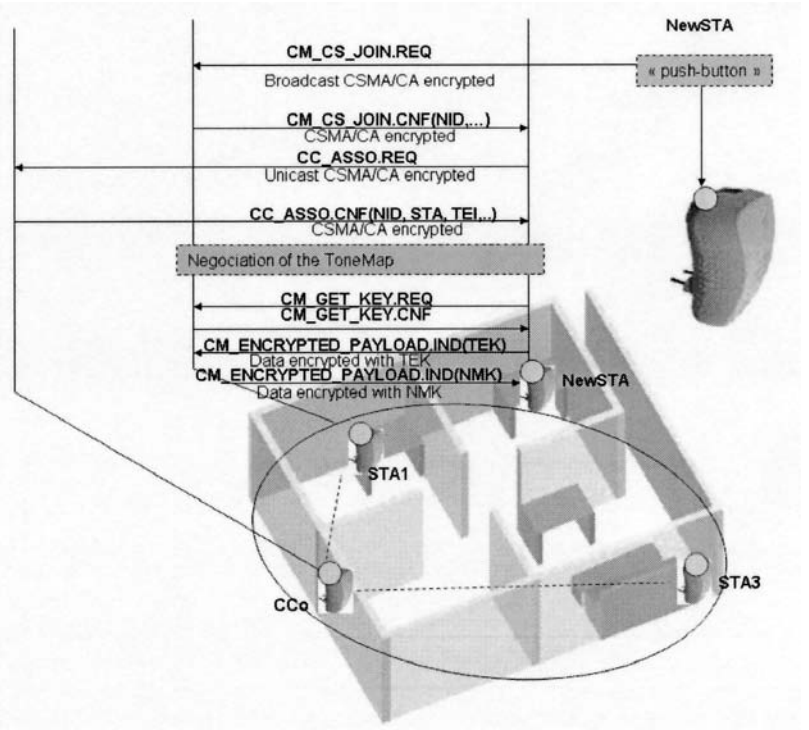

Figure 9.10 HomePlug AV PLC device association principle with the EasyConnect mode

As a configuration example, we are going to use the tool developed by AsokaUSA for its easy implementation and its user-friendly user interface. Once the Power Manager tool is started, it offers a choice of network interfaces which will be used by the program as illustrated in Figure 9.11.

The installation program then starts with the installation of the driver required for good operation of the frames sent to the PLC devices as illustrated in Figure 9.12.

Once the installation program is started, it carries out several steps until the installation of the Power Manager PLC tool is completed (see complete Figure 9.13).

Once the installation is completed, the Power Manager tool prompts to rename the PLC device to which the installation PC is connected (see Figure 9.14) and to

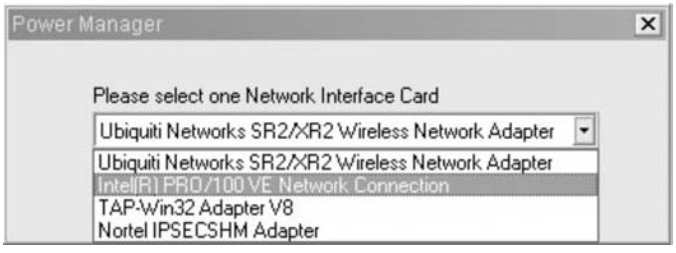
Power Manager
Please select one Network Interface Card
Ubiquiti Networks SR2/XR2 Wireless Network Adapter
Ubiquiti Networks SR2/XR2 Wireless Network Adapter
Intel(R) PRO/100 VE Network Connection
TAP-Win32 Adapter V8
Nortel IPSECSHM Adapter

Figure 9.11 Network interface choice

Figure 9.12 PLC tool module installation choice

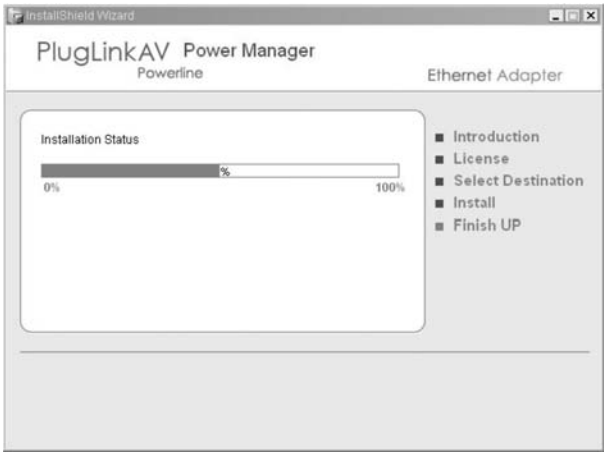

Figure 9.13 PLC tool installation progress

assign a device name to it that will be used for easily retrieving the identity of this device in the PLC logical network supervision.

At that level, the NEK used for all the PLC devices of the logical PLC network we want to configure can then be configured. Here, as illustrated in Figure 9.15, we use the HomePlug123 NEK.

The PLC tool main interface then opens with various possible icons for managing the device profiles, the devices existing on the logical network, the updating of firmware versions, and statistics of PLC links between devices as illustrated in Figure 9.16.

In the "Devices" tab, it is then possible simply to view the configured device or devices and to indicate new parameters to them, like their name or NEK, as illustrated in Figure 9.17.

The NEK can also be indicated on a remote device on the electrical network using the DEK in the case of the PLC remote device as indicated in Figure 9.18.

InstallShield Wizard
Set up Local Device Name
Currently, your local device name is PlugLink(local). This option allows you to change the device into a different name so you can distinguish the devices within your home. For example, living room unit, master bedroom unit, etc. This is an optional feature for advanced users only. We recommend you use the default settings and click next.
Do you want to change the local device name?
Select one below:
Yes
No
Enter new local device name here
MyPLCDevice1
Cancel
Next

Figure 9.14 Renaming of local PLC device connected to the configuration PC

InstallShield Wizard
Set up Local Device Network Password
Currently, your local device network password is HomePlugAV. This option allows you to change the device network password. For example, John, Fish, etc. This is an optional feature for advanced users only. We recommend you use the default settings and click next.
Do you want to change the local device Network Password?
Select one below:
Yes
No
Enter new Network Password here
HomePlug123
Back
Cancel
Next

Figure 9.15 NEK configuration for PLC logical network

With all the functionalities of the Power Manager tool, it is then possible to install, configure, and supervise a HomePlug AV network easily by following the installation rules previously stated in Chapters 7 and 8.

Configuring a HomePlug 1.0 PLC Network Under Linux

In the same manner as under Windows, installing a PLC network under Linux consists in connecting the network interface card of the PC to one of the PLC devices of the electrical network and in using a PLC configuration tool for Linux.

In the case of a PLC device with a USB interface, the driver of the Ethernet USB virtual interface must be installed. For this purpose, it is necessary to recover the record containing this driver by downloading it at the following address (for a Devolo device):

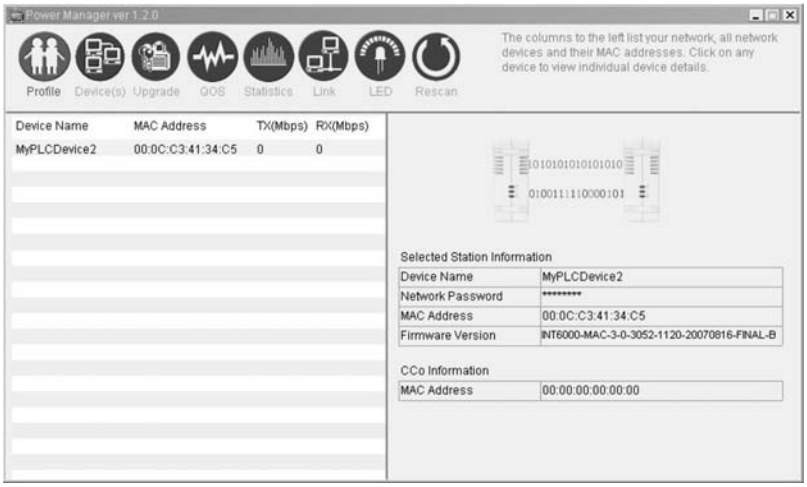

Figure 9.16 Power Manager tool main tab

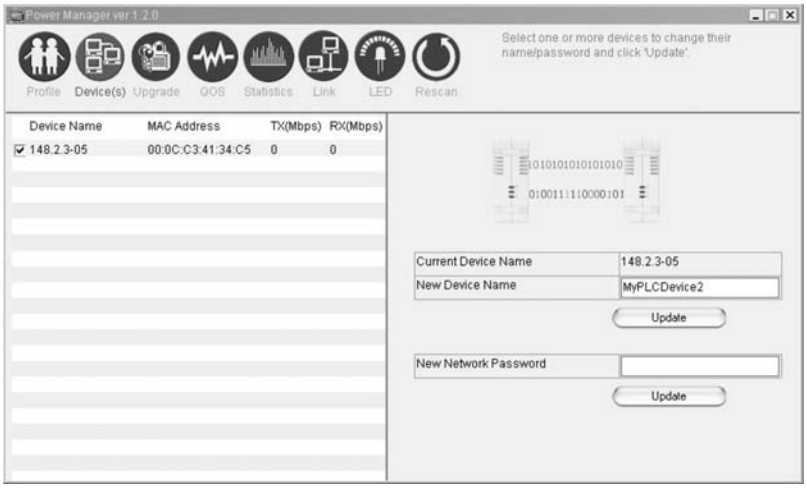

Figure 9.17 Power Manager tool "Devices" tab

http://download.devolo.biz/webcms/0607105001130251610/dLAN-linux-package-2.0.tar.gz

Figure 9.19 illustrates the page of the Devolo site offering PLC configuration tools for dLAN duo devices.

Just click on the Driver Linux link to download it, then save the file at a location on the disk when the downloading window illustrated in Figure 9.20 is displayed.

In our example, we save the file under:

```
carcelle@debian:~/Projects/CPL
```

Once the file is downloaded, it must be decompressed twice with the following commands:

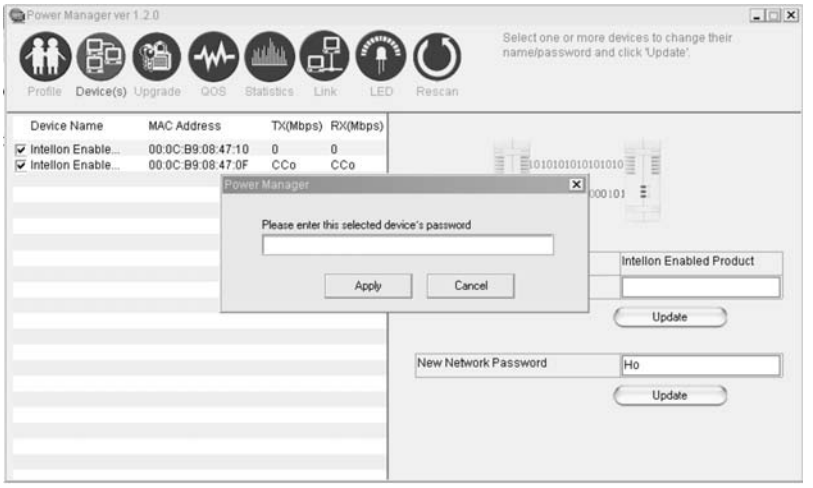

Figure 9.18 DEK key configuration for a remote device

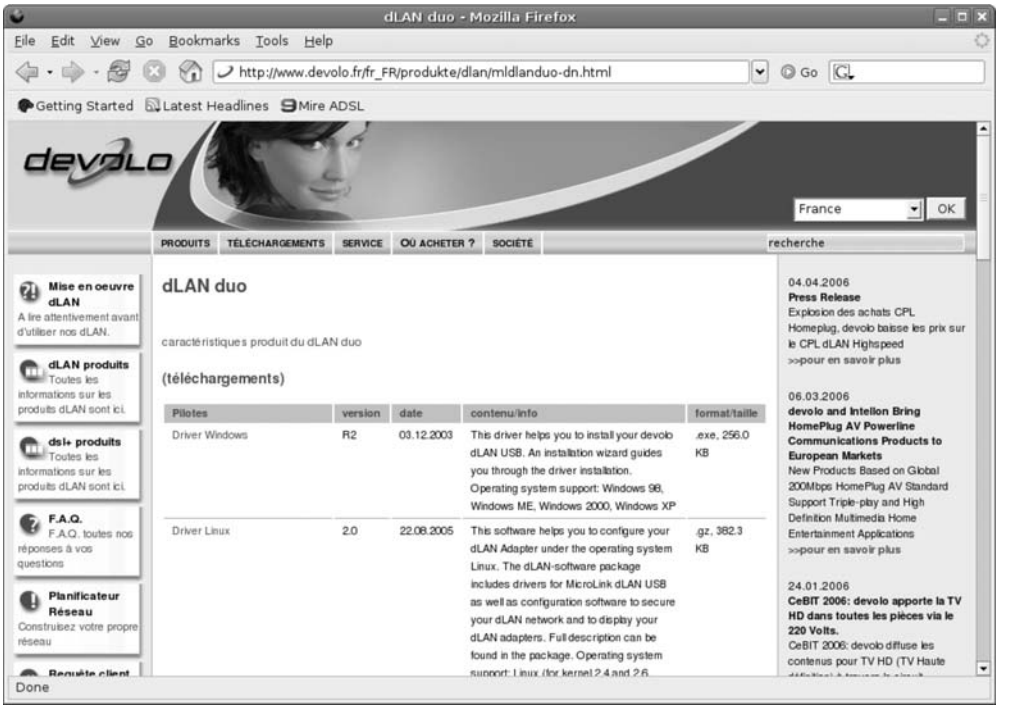

Figure 9.19 Homepage for Devolo dLAN duo device configuration tools

```
carcelle@debian:~/Projects/CPL$gunzip dLAN-linux-pack-
age-2.0.tar.gz
carcelle@debian:~/Projects/CPL$gunzip dLAN-linux-pack-
age-2.0.tar.gz
```

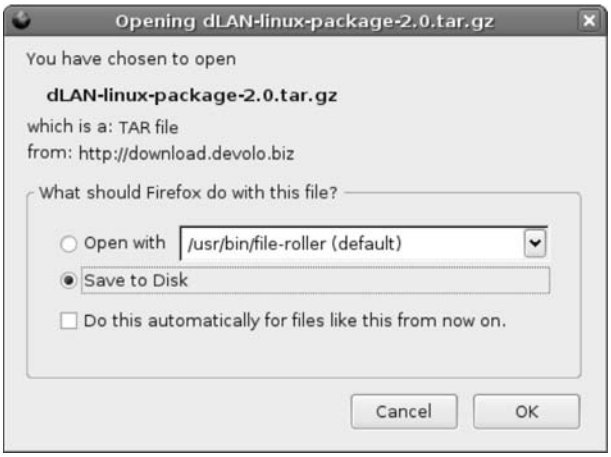

Figure 9.20 Linux PLC tool downloading window

The USB PLC device must then be connected to an available port of the PC and the device recognition must be verified by running the following command:

```
carcelle@debian:~/Projects/CPL$dmesg
```

The dmesg command gives the output illustrated in Figure 9.21.

The directory in which the PLC tool was decompressed must be opened to install the driver downloaded in this way:

```
carcelle@debian:~/Projects/CPL$cd dLAN-linux-package-2.0/driver/
```

Figure 9.22 illustrates the files contained in this directory.

From that moment, it is necessary to switch over to super user (root) mode and then run the install.boot.sh installation command shown in Figure 9.23.

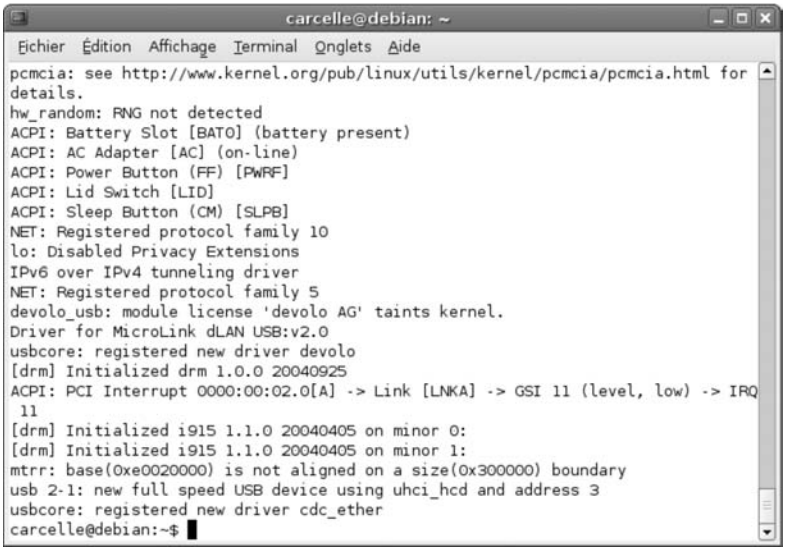
carcelle@debian: ~
Fichier Édition Affichage Terminal Onglets Aide
pcmcia: see http://www.kernel.org/pub/linux/utils/kernel/pcmcia/pcmcia.html for details.
hw_random: RNG not detected
ACPI: Battery Slot [BAT0] (battery present)
ACPI: AC Adapter [AC] (on-line)
ACPI: Power Button (FF) [PWRF]
ACPI: Lid Switch [LID]
ACPI: Sleep Button (CM) [SLPB]
NET: Registered protocol family 10
lo: Disabled Privacy Extensions
IPv6 over IPv4 tunneling driver
NET: Registered protocol family 5
devolo_usb: module license 'devolo AG' taints kernel.
Driver for MicroLink dLAN USB:v2.0
usbcore: registered new driver devolo
[drm] Initialized drm 1.0.0 20040925
ACPI: PCI Interrupt 0000:00:02.0[A] -> Link [LNKA] -> GSI 11 (level, low) -> IRQ 11
[drm] Initialized i915 1.1.0 20040405 on minor 0:
[drm] Initialized i915 1.1.0 20040405 on minor 1:
mtrr: base(0xe0020000) is not aligned on a size(0x300000) boundary
usb 2-1: new full speed USB device using uhci_hcd and address 3
usbcore: registered new driver cdc_ether
carcelle@debian:~$

Figure 9.21 Dmesg command output

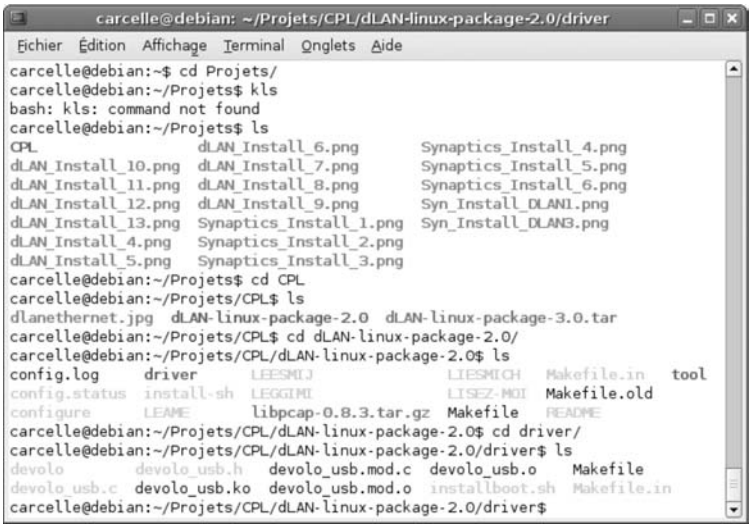

Figure 9.22 Contents of USB PLC device driver directory

To compile the USB driver, the next make usbdriver command must then be run (see Figure 9.24):

```
carcelle@debian:~/Projects/CPL/dLAN-linux-package-2.0/driver$make
usbdriver
```

Once the compilation is completed, the next command, illustrated in Figure 9.25, is used for installing the driver at the suitable disk locations (see Figure 9.26):

```
carcelle@debian:~/Projects/CPL/dLAN-linux-package-2.0/driver$make
install-usbdrive
```

Lastly, the next command:

Figure 9.23 Running the installation command

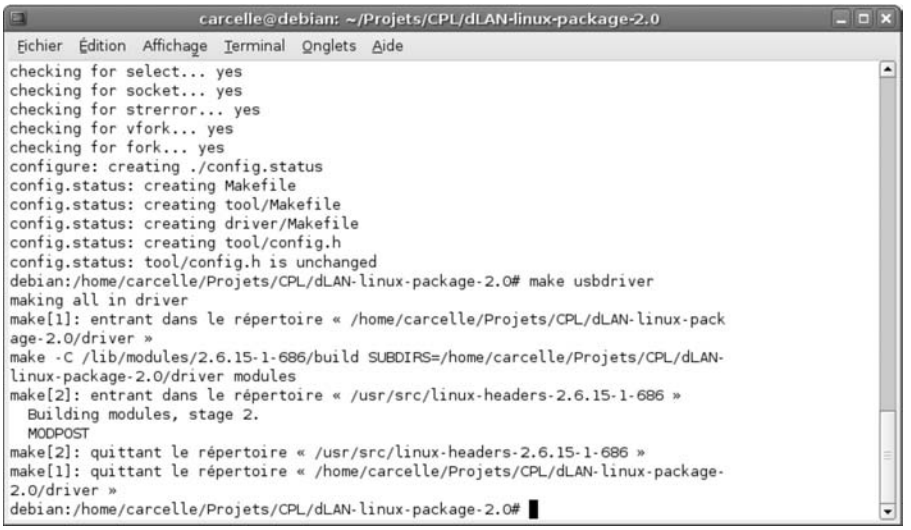

Figure 9.24 Running the make usbdriver command

carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0
Fichier Édition Affichage Terminal Onglets Aide
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-pack
age-2.0/driver »
make -C /lib/modules/2.6.15-1-686/build SUBDIRS=/home/carcelle/Projets/CPL/dLAN-
linux-package-2.0/driver modules
make[2]: entrant dans le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
Building modules, stage 2.
MODPOST
make[2]: quittant le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-
2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install-usbdriver
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko /lib/modules
/2.6.15-1-686/extra
/sbin/depmod -a && /sbin/modprobe devolo_usb
In order to have your usb driver running and configured
at boot, you should go into driver directory and type
make installboot
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0#

Figure 9.25 Running the make install-usbdriver command

```
carcelle@debian:~/Projects/CPL/dLAN-linux-package-2.0/driver$make
installboot
```

enables the USB driver to be loaded when starting up.

Simply reboot the computer to validate all the commands.

Once rebooting is completed, the device must still be connected to the USB port in order to make sure that the new USB Ethernet virtual board is installed as illustrated in Figure 9.27.

The dlanusb0 board is actually installed. We can start installing the configuration utility.

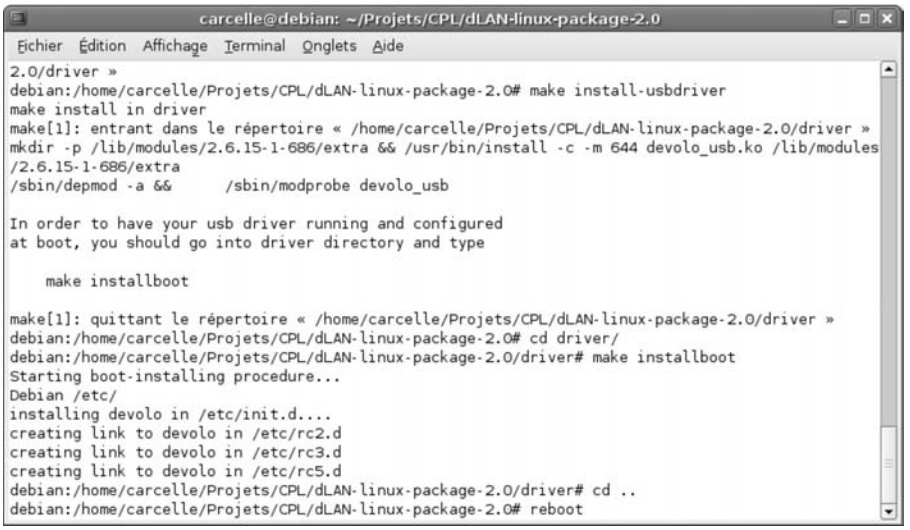
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0
Fichier Édition Affichage Terminal Onglets Aide
2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install-usbdriver
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko /lib/modules
/2.6.15-1-686/extra
/sbin/depmod -a && /sbin/modprobe devolo_usb
In order to have your usb driver running and configured
at boot, you should go into driver directory and type
make installboot
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# cd driver/
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver# make installboot
Starting boot-installing procedure...
Debian /etc/
installing devolo in /etc/init.d....
creating link to devolo in /etc/rc2.d
creating link to devolo in /etc/rc3.d
creating link to devolo in /etc/rc5.d
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver# cd ..
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# reboot

Figure 9.26 Running the make install-boot command

carcelle@debian: ~
Fichier Édition Affichage Terminal Onglets Aide
carcelle@debian:~$ sudo ifconfig -a
dlanusb0 Link encap:Ethernet HWaddr 00:0B:3B:0D:6A:89
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
eth0 Link encap:Ethernet HWaddr 00:0A:E4:37:7C:E5
inet6 addr: fe80::20a:e4ff:fe37:7ce5/64 Scope:Link
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:5 errors:0 dropped:0 overruns:0 frame:0
TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:460 (460.0 b) TX bytes:2776 (2.7 KiB)
eth1 Link encap:Ethernet HWaddr 00:12:F0:E9:CB:F9
inet addr:192.168.10.100 Bcast:192.168.10.255 Mask:255.255.2
55.0
inet6 addr: fe80::212:f0ff:fee9:cbf9/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1661 errors:0 dropped:40 overruns:0 frame:0
TX packets:1618 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1359910 (1.2 MiB) TX bytes:376023 (367.2 KiB)
Interrupt:11 Base address:0xe000 Memory:d0200000-d0200fff
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:154 errors:0 dropped:0 overruns:0 frame:0
TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:10040 (9.8 KiB) TX bytes:10040 (9.8 KiB)
sit0 Link encap:IPv6-in-IPv4

Figure 9.27 Making sure that the Ethernet/USB virtual board is installed

Since the configuration tool under Linux has been decompressed in the same directory as the USB driver, it must first of all be placed it in the correct directory:

```
debian:home/carcelle/Projects/CPL/dLAN-linux-package-2.0#./con-
figure
```

We can start by configuring the compilation parameters as illustrated in Figure 9.28.

The compilation of the PLC configuration tool can be started using the make command as illustrated in Figure 9.29.

Once the compilation has been completed, the compiled files must be installed in the correct disk locations using the make install command.

The configuration tool can then be run with the Ethernet/USB virtual board or with the Ethernet board connected to a USB PLC or Ethernet device using the following command (see Figure 9.30):

```
carcelle@debian:~/Projects/CPL/dLAN-linux-package-2.0$sudo
dlanconfig eth0
```

The tool can be run on the eth0 or dlanusb0 interface. Figure 9.31 illustrates the sensing of PLC devices connected to the PLC network performed by the configuration tool.

In this example, the sensed PLC device corresponds to the HomePlug 1.0 specification since its estimated physical data rate is around 12.829 Mbit/s.

A menu with the four following functionalities is proposed by the configuration tool:

carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0
Fichier Édition Affichage Terminal Onglets Aide
dLAN-linux-package-2.0/LIESMICH
dLAN-linux-package-2.0/LISEZ-MOI
dLAN-linux-package-2.0/README
debian:/home/carcelle/Projets/CPL# clear
debian:/home/carcelle/Projets/CPL# cd dLAN-linux-package-
dLAN-linux-package-2.0/ dLAN-linux-package-3.0.tar
debian:/home/carcelle/Projets/CPL# cd dLAN-linux-package-2.0/
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ls
configure install-sh LEESMIJ libpcap-0.8.3.tar.gz LISEZ-MOI README
driver LEAME LEGGIMI LIESMICH Makefile.in tool
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ./configure
checking for gcc... gcc
checking for C compiler default output... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking gcc version... 4
checking maximum warning verbosity option... -Wall for C
checking for a BSD-compatible install... /usr/bin/install -c
checking whether ln -s works... yes
checking for modprobe... /sbin/modprobe
checking for module_prefix... /lib/modules
checking for depmod... /sbin/depmod
USB determination method: /bin/lspci -v
USB driver to be loaded: uhci
checking what kind of binaries we shall create... dynamically linked
checking for library containing gethostbyname... none required
checking for library containing socket... none required
checking for library containing putmsg... none required
checking for local pcap library... not found

Figure 9.28 Configuring the compilation parameters

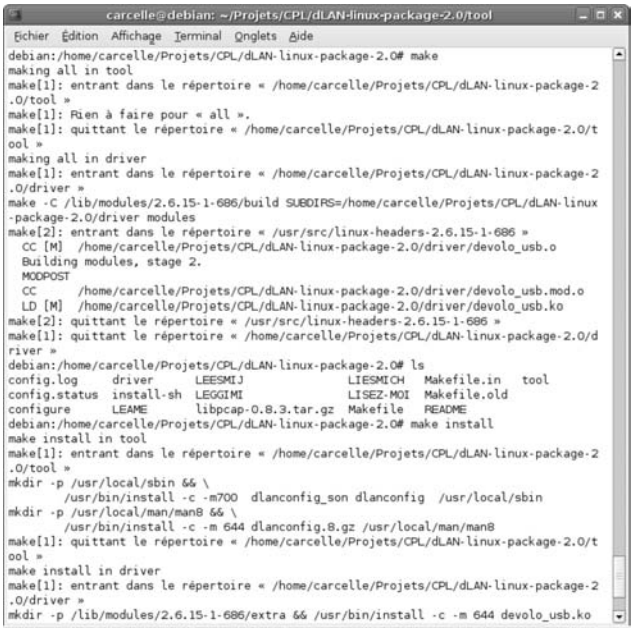
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0/tool
Fichier Édition Affichage Terminal Onglets Aide
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make
making all in tool
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/tool »
make[1]: Rien à faire pour « all ».
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/tool »
making all in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
make -C /lib/modules/2.6.15-1-686/build SUBDIRS=/home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver modules
make[2]: entrant dans le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
CC [M] /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.o
Building modules, stage 2.
MODPOST
CC /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.mod.o
LD [M] /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.ko
make[2]: quittant le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ls
config.log driver LEESMIJ LIESMICH Makefile.in tool
config.status install-sh LEGGIMI LISEZ-MOI Makefile.old
configure LEAME libpcap-0.8.3.tar.gz Makefile README
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install
make install in tool
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/tool »
mkdir -p /usr/local/sbin && \
/usr/bin/install -c -m700 dlanconfig_son dlanconfig /usr/local/sbin
mkdir -p /usr/local/man/man8 && \
/usr/bin/install -c -m 644 dlanconfig.8.gz /usr/local/man/man8
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/tool »
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko

Figure 9.29 Compiling the PLC configuration tool

carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0/tool
Fichier Édition Affichage Terminal Onglets Aide
-package-2.0/driver modules
make[2]: entrant dans le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
CC [M] /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.o
Building modules, stage 2.
MODPOST
CC /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.mod.o
LD [M] /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.ko
make[2]: quittant le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ls
config.log driver LEESMIJ LIESMICH Makefile.in tool
config.status install-sh LEGGIMI LISEZ-MOI Makefile.old
configure LEAME libpcap-0.8.3.tar.gz Makefile README
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install
make install in tool
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/tool »
mkdir -p /usr/local/sbin && \
/usr/bin/install -c -m700 dlanconfig_son dlanconfig /usr/local/sbin
mkdir -p /usr/local/man/man8 && \
/usr/bin/install -c -m 644 dlanconfig.8.gz /usr/local/man/man8
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/tool »
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko
/lib/modules/2.6.15-1-686/extra
/sbin/depmod -a && /sbin/modprobe devolo_usb
In order to have your usb driver running and configured
at boot, you should go into driver directory and type
make installboot
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0#

Figure 9.30 Installing the PLC configuration tool

- "set local network password," used for configuring the PLC network key (NEK) on the PLC device or devices directly connected to the configuration PC using Ethernet;

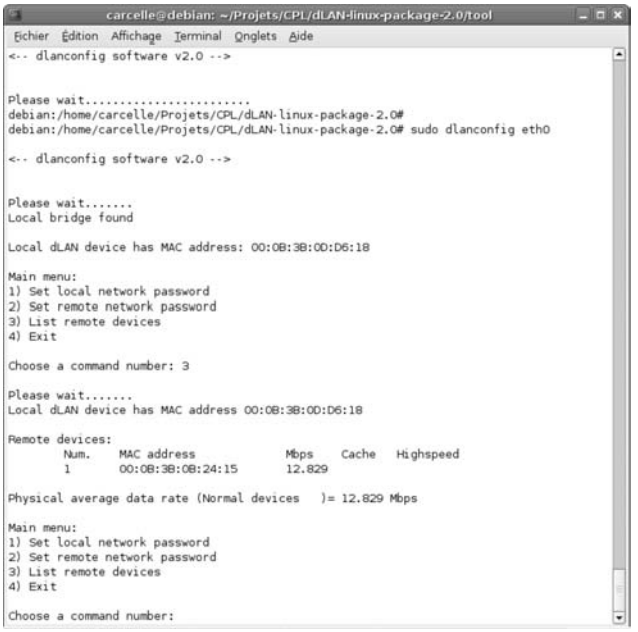

Figure 9.31 Sensing of an Ethernet PLC device using the Linux PLC configuration tool

- "set remote network password," used for configuring the PLC network key on remote PLC devices connected to the electrical network (DEK);
- "list remote devices," which is used for listing the PLC devices connected to the PLC network and configured with the same PLC network key;
- "exit," used for exiting the configuration tool.

Configuring a HomePlug AV PLC Network Under Linux

Concerning HomePlug AV PLC devices, there are not many tools under Linux adapted to usual network environments for 802.11, BlueTooth, and 802.16 (soon) network technologies. However, there is an integrated PLC tool in the form of a library and package to distribute the available Debian (.deb packet) and RedHat (.rpm packet) packages:

- FAIFA (Developed by Florian Fainelli, Nicolas Thill, and Xavier Carcelle) which is available at the project address: http://open-plc.org/

  The http://open-plc.org/ site groups a certain amount of information on PLC technologies and compatibilities between devices and firmware for the HomePlug AV standard.

  The FAIFA tool can be downloaded from the following addresses.

  The installation can be done in different ways:
- Compilation of the project sources under a Linux distribution used by the user from the tarball available at the following address:

  http://svn.open-plc.org/

after performing a check-out on the development repository using the following command:

```
#svn co http://svn.open-plc.org/
```

- Installation of the Debian faifa.deb package from the debian.open-plc.org repository by adding this line in the /etc/apt/sources.list file:
  http://deb.open-plc.org
- Installation of the RedHat faifa.rpm package from the following link:
  http://rpm.open-plc.org
- Once the FAIFA tool is compiled and installed, it enables access to the functions useful for the configuration:
  - Configuration of NEK keys on the logical network PLC devices;
  - Discovery of the devices existing on this logical network;
  - Statistics retrieval for links between PLC devices.

When the user starts FAIFA with the command line below:

```
#./faifa –i eth0 –m
```

Where the option
- –i: indicates the network interface to be used for accessing the PLC network;
- –m: tells FAIFA to display the menu.

When the FAIFA menu is started up, it displays the menu below:

```
Faifa for HomePlug AV

Started receive thread

Supported HomePlug AV frames

type   description
----   -----------
0xA000 Get Device/SW Version Request
0xA030 Get Link Statistics Request
0xA038 Network Info Request (Vendor-Specific)
0xA050 Set Encryption Key Request
0xA054 Get Manufacturing String Request

Supported HomePlug 1.0 frames

type   description
----   -----------
0x0000 Channel Estimation Request
0x0004 Set Network Encryption Key Request
0x0007 Parameters and Statistics Request
0x0019 Set Local parameters Request
0x001D Set Local Overrides Request

Choose the frame type (Ctrl-C to exit):
```

One of the options among the two submenus for the HomePlug AV and 1.0/Turbo standards can then be chosen. When the user chooses the 0xA000

option, he or she obtains the information on the firmware versions available on the Intellon chip as illustrated below:

```
Choose the frame type (Ctrl-C to exit): 0xa000

Init:
Frame: Get Device/SW Version Request (0xA000)
Binary Data, 60 bytes
00000000: 00 B0 52 00 00 01 00 00 00 00 00 88 E1 00 00
00000016: A0 00 B0 52 00 00 00 00 00 00 00 00 00 00 00
00000032: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048: 00 00 00 00 00 00 00 00 00 00 00 00

Dump:
Frame: Get Device/SW Version Confirm (A001), HomePlug-AV Version:
1.0
Status: Success
Device ID: INT6300, Version: INT6000-MAC-3-1-3103-1662-20070915-
FINAL-B, upgradeable: 0
Binary Data, 156 bytes
00000000: 00 00 00 00 00 00 0C B9 08 47 0F 88 E1 00 01
00000016: A0 00 B0 52 00 02 2A 49 4E 54 36 30 30 30 2D 4D
00000032: 41 43 2D 33 2D 31 2D 33 31 30 33 2D 31 36 36 32
00000048: 2D 32 30 30 37 30 39 31 35 2D 46 49 4E 41 4C 2D
00000064: 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000096: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000112: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000128: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000144: 00 00 00 00 00 00 00 00 00 00 00 00
```

When the user chooses the 0xA038 option, the FAIFA program sends back information on the other devices existing on the logical PLC network as well as a number of statistics in the HomePlug AV standard as illustrated below:

```
Choose the frame type (Ctrl-C to exit): 0xa038

Init:
Frame: Network Info Request (Vendor-Specific) (0xA038)
Binary Data, 60 bytes
00000000: 00 B0 52 00 00 01 00 00 00 00 00 88 E1 00 38
00000016: A0 00 B0 52 00 00 00 00 00 00 00 00 00 00 00
00000032: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048: 00 00 00 00 00 00 00 00 00 00 00 00

Dump:
Frame: Network Info Confirm (Vendor-Specific) (A039), HomePlug-AV
Version: 1.0
Network ID (NID): B0 F2 E6 95 66 6B 03
Short Network ID (SNID): 0x0e
STA TEI: 0x01
STA Role: Station
CCo MAC:
        00:0C:B9:08:47:10
CCo TEI: 0x03
Stations: 1
Station MAC       TEI  Bridge MAC        TX   RX
-----------       ---  ----------        --   --
00:0C:B9:08:47:10 0x03 FF:FF:FF:FF:FF:FF 0x00 0x00
Binary Data, 60 bytes
```

```
00000000: 00 00 00 00 00 00 00 0C B9 08 47 0F 88 E1 00 39
00000016: A0 00 B0 52 01 B0 F2 E6 95 66 6B 03 0E 01 00 00
00000032: 0C B9 08 47 10 03 01 00 0C B9 08 47 10 03 FF FF
00000048: FF FF FF FF 00 00 00 00 00 00 00 00
```

Finally, the 0xA054 option is used for obtaining information on the PLC device manufacturer and a number of statistics on the PLC logical links between the network devices.

```
Choose the frame type (Ctrl-C to exit): 0xa054

Init:
Frame: Get Manufacturing String Request (0xA054)
Binary Data, 60 bytes
00000000: 00 B0 52 00 00 01 00 00 00 00 00 00 88 E1 00 54
00000016: A0 00 B0 52 00 00 00 00 00 00 00 00 00 00 00 00
00000032: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048: 00 00 00 00 00 00 00 00 00 00 00 00

Dump:
Frame: Get Manufacturing String Confirm (A055), HomePlug-AV
Version: 1.0
Status: Success
Length: 64 (0x40)
Manufacturer string: Intellon HomePlug AV Device
Binary Data, 86 bytes
00000000: 00 00 00 00 00 00 00 0C B9 08 47 0F 88 E1 00 55
00000016: A0 00 B0 52 00 40 49 6E 74 65 6C 6C 6F 6E 20 48
00000032: 6F 6D 65 50 6C 75 67 20 41 56 20 44 65 76 69 63
00000048: 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000064: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080: 00 00 00 00 00 00

Dump:
Frame: Get Link Statistics Confirm (A031), HomePlug-AV
Version: 1.0
Status: Success
Link ID: fc
TEI: 00
Direction: Tx
MPDU acked.....................: 1249
MPDU collisions................: 271
MPDU failures..................: 0
PB transmitted successfully.....: 1628
PB transmitted unsuccessfully...: 0
Direction: Rx
MPDU acked.....................: 886
MPDU failures..................: 0
PB received successfully........: 1539
PB received unsuccessfully......: 0
Turbo Bit Errors passed.........: 241
Turbo Bit Errors failed.........: 0
-- Rx interval 0 --
Rx PHY rate.....................: 93
PB received successfully........: 17
PB received failed..............: 0
TBE errors over successfully....: 26
TBE errors over failed..........: 0
-- Rx interval 1 --
Rx PHY rate.....................: 93
PB received successfully........: 15
```

```
PB received failed.............: 0
TBE errors over successfully....: 21
TBE errors over failed..........: 0
-- Rx interval 2 --
Rx PHY rate.....................: 93
PB received successfully........: 26
PB received failed..............: 0
TBE errors over successfully....: 47
TBE errors over failed..........: 0
-- Rx interval 3 --
Rx PHY rate.....................: 93
PB received successfully........: 14
PB received failed..............: 0
TBE errors over successfully....: 50
TBE errors over failed..........: 0
-- Rx interval 4 --
Rx PHY rate.....................: 93
PB received successfully........: 25
PB received failed..............: 0
TBE errors over successfully....: 38
TBE errors over failed..........: 0
-- Rx interval 5 --
Rx PHY rate.....................: 93
PB received successfully........: 24
PB received failed..............: 0
TBE errors over successfully....: 59
TBE errors over failed..........: 0
```

Configuring a PLC Network Under FreeBSD

The FreeBSD operating system does not provide many tools for configuring PLC networks. We are going to detail the plconfig program, which is one of the only programs currently available for this type of platform.

FreeBSD is an operating system similar to Linux, originating from work on Unix kernels carried out within Berkeley University in California. Although there are few differences compared to Linux distributions, developments carried out on a FreeBSD platform slightly differ.

The FreeBSD operating system is mainly used by security, Web, and mail servers. FreeBSD uses a packets system, called "ports," representing programs that can be used under this operating system. This ports system is managed by a group of developers distributed worldwide ensuring its integrity. The number of these developers is much less important than for Linux, which makes FreeBSD both more stable and more homogeneous.

Let us first download Manuel Kasper's tool, plconfig, at the following address: https://neon1.net/prog/plconfig-0.2.tar.gz.

On a console in super user mode, we decompress the tool installation program, then start the installation using the make command.

The program displays a help menu if no network interface or option is indicated as a parameter for the plconfig command:

```
#tar xfvz plconfig-0.2.tar.gz; cd plconfig-0.2
#make
#./plconfig
Syntax
```

```
Powerline Bridge config version 0.2 by Manuel Kasper
<mk@neon1.net>

Usage:   plconfig [-pqrh] [-b device] [-s key] interface

         -s key            set network encryption key
                           (plaintext password or 8 hex bytes
preceded by 0x)
         -b device         use device (default is /dev/bpf0)
         -p                don't switch interface to promiscuous
mode
         -r                request parameters and statistics
         -q                request Intellon-specific network
statistics
         -h                display this help

         If -s is not specified, plconfig will listen for
management packets indefinitely (after requesting stats if -r is
specified)
```

As indicated in this help menu, the following PLC network functionalities are proposed by the program:

- –s: used for configuring the NEK on devices locally connected to the configuration PC using Ethernet.
- –r: used for interrogating the HomePlug chip of the locally connected PLC device and retrieving a number of parameters and statistics. This option is also used for displaying the electrical network PLC devices that are correctly configured.
- –q: used for interrogating the PLC chip and retrieving values and statistics specific to the manufacturer of Intellon chips.

As we can see, the program is not as complete as tools under Windows or Linux but nonetheless offers the main functionalities required to configure a PLC network (network key configuration and status of the PLC links at a physical level).

Configuring an HD-PLC Network

The HD-PLC standard was developed by Panasonic, which markets HD-PLC devices mainly in Japan under the BL-PA300 (PL-HNC-006) P/N reference running on 110V/50 to 60 Hz. The HD-PLC standard operates in network mode of the master-slave type with a network device in master mode (configured using a button on the device) and the other devices in slave mode (also configured using a button on the devices). The embedded software on HD-PLC devices (based on an ARM926-EJS hardware architecture and a μITRON OS, with a PX-PRP1A9-4 reference) has three main components:

- *The IP stack and HTTPD:* The devices are configured using an embedded WEB interface on HD-PLC devices.
- *The DataLink stack:* Used for managing the PLC interface, the ETHERNET interface, and the SERIAL interface.

- *The Tasks Communications stack:* Used with mails and events for tasks communication, interrupt handlers, and buffers for exchanging information with the hardware interface.

Configuring a DS2 Network

The Spanish manufacturer DS2 is a player on the HomePlug market whose products are not compatible with HomePlug devices.

A DS2 200-Mbit/s PLC network is locally configured on the device via an HTTP interface. Therefore, it is identical for Windows and for Linux/FreeBSD.

The DS2 devices can operate in three different network modes:

- *HE:* The device is the PLC network master.
- *CPE:* The device is the PLC network slave.
- *TDREP:* The device is used as the PLC network repeater.

We will illustrate this section with Corinex AV PLC devices based on DS2 Wisconsin chips. There are two firmware types in these devices: alma and spirit. We have chosen a device with alma firmware, which offers more functionalities.

Before connecting to the HTTP interface, the PLC device and the configuration PC must be placed in the same IP addressing plane. Since the default IP address of Corinex AV PLC devices is 10.10.1.69, the IP address of the configuration PC must be configured in the same addressing plane, for example, 10.10.1.10.

Figure 9.32 illustrates the various addressing planes that will coexist on the electrical network.

Once you are connected to the homepage, enter the default password (paterna) to open the configuration pages as illustrated in Figure 9.33.

The first configuration page offers an overview of the main parameters of a DS2 PLC device (see Figure 9.34), in particular the following ones:

- IP address of the PLC device;
- MAC network mode (HE, CPE, TDREP) of the PLC device;
- PLC physical link mode;
- Multicast groups at the IP layer level;
- Key (or password) used for securing the PLC network;
- Priorities of some data flows between PLC devices.

These parameters can be configured separately then validated and written into the computer's nonvolatile memory. The modifications made to the overall configuration are taken into account by rebooting the device.

The IP address, the subnet mask, and the default gateway of the device can be configured by clicking on "Change configuration" below "Default Gateway IP Address." The configuration page illustrated in Figure 9.35 is then displayed.

In the example of Figure 9.36, the addresses of the PLC1, PLC2, and PLC3 devices are 10.10.1.1, 10.10.1.2, and 10.10.1.3, respectively, and the subnet mask is

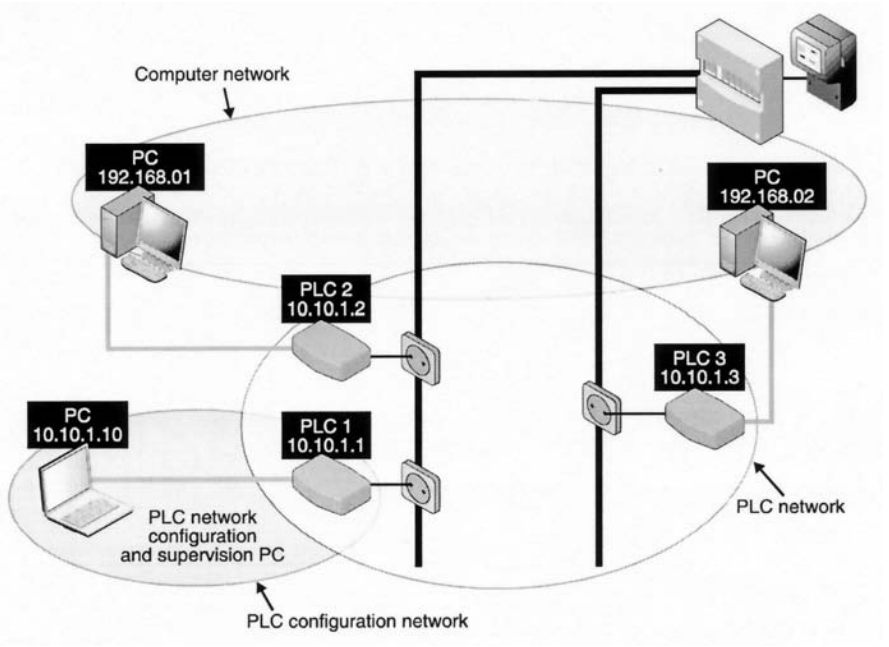

Figure 9.32 Addressing planes of a DS2 PLC network

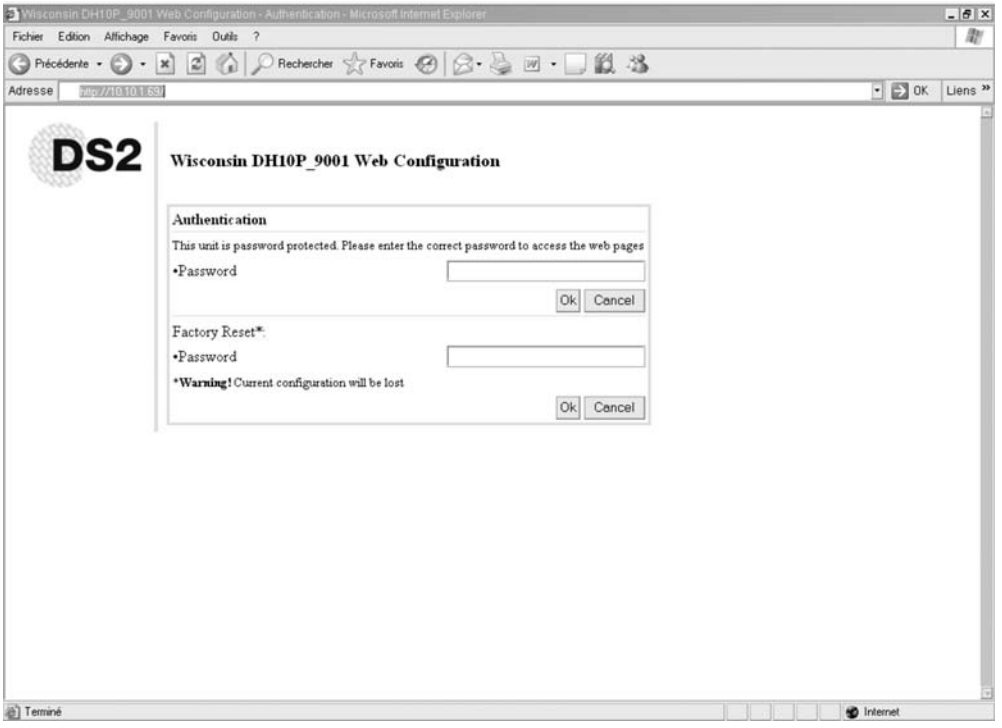

Figure 9.33 DS2 configuration HTTP tool homepage

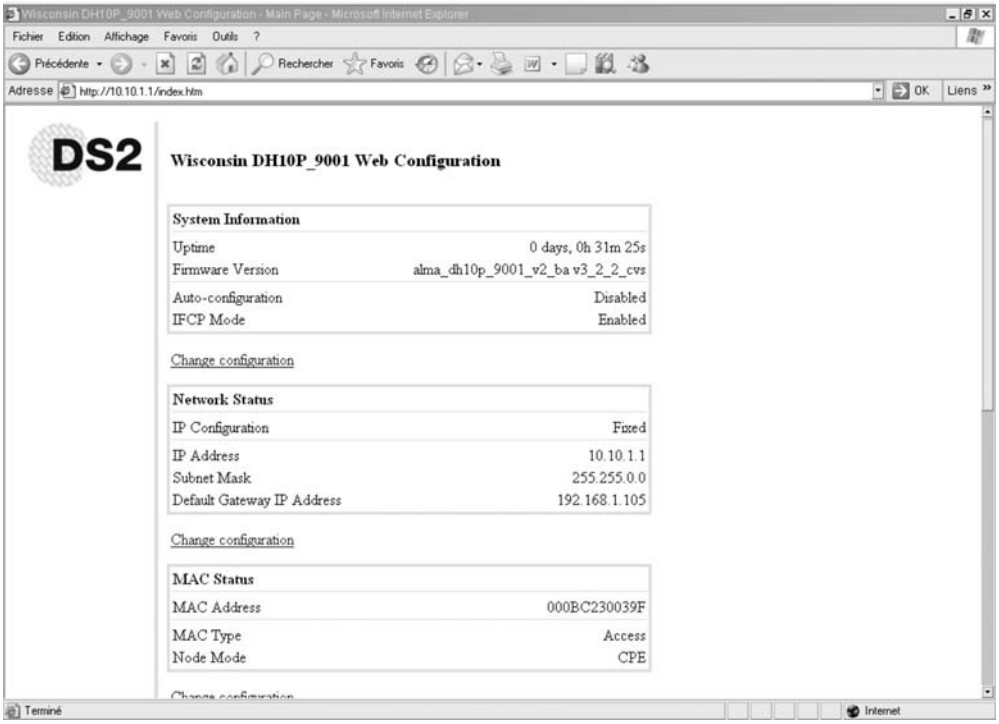

Figure 9.34 DS2 PLC device configuration parameters

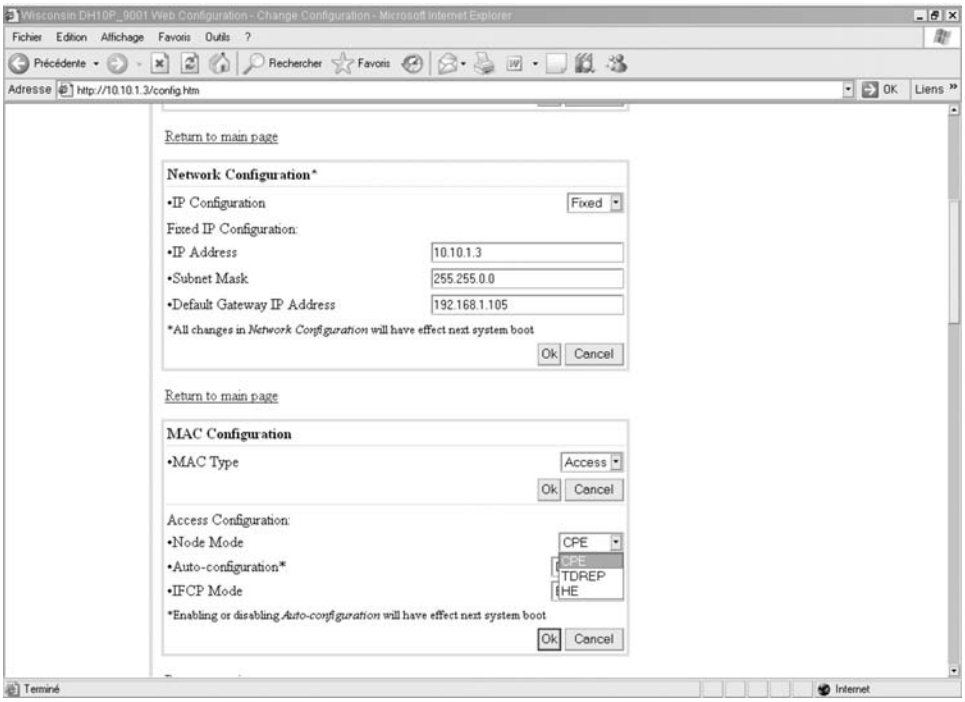

Figure 9.35 DS2 PLC device MAC and network parameters configuration

placed at 255.255.0.0. In this case, the default gateway is not important since the configuration PC has an address in the same addressing plane (10.10.1.10).

Once these network parameters are configured, it is important to configure the network mode for each PLC device.

As illustrated by Figure 9.36, the device closest to the circuit breaker panel is in master (HE) mode; the other devices are in slave (CPE) or repeater (TDREP) mode. The repeater mode is used for reaching devices that cannot be easily connected due to the length of the electrical wiring or to other electrical environment constraints the building may have.

This configuration is performed in the Access configuration section of the MAC configuration window pane by selecting Node Mode. A window then prompts you to choose among the three possible modes.

Groups of multicast IP type can be created with DS2 PLC devices and IP frames are sent from a source device to several destination devices belonging to the multicast group. To implement groups of "multicast" IPs, it is important to have good knowledge of the configuration techniques for IP networks (see end of chapter).

One of the essential parameters of any type of PLC networks is the network key, called "password" in the DS2 configuration tool; it is used for creating private PLC networks and securing data frame exchanges between network components (devices and terminals connected to the PLC network). This is done in the "Security Configuration" section (see Figure 9.37) by entering the new password of the PLC network specific to this network. This parameter is the equivalent of the NEK for HomePlug PLC networks.

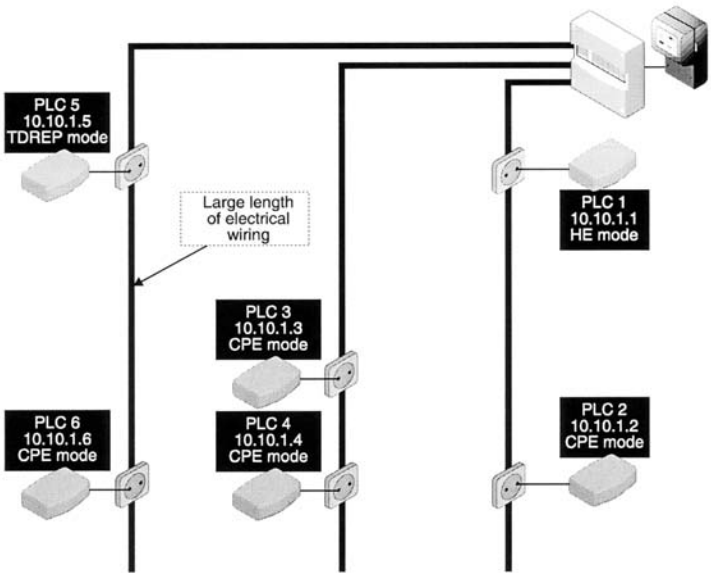

Figure 9.36 DS2 PLC device network mode configuration

The priority of each of the network PLC devices can then be configured by setting the "Default priority" parameter of the "Priority configuration" section from 1 to 5 according to the network topology and the function of each device.

For example, based on the topology of Figure 9.37, the device in master mode can be configured with a "higher" priority level (value 1), and some PLC devices in CPE mode with an "average" priority level (value 2) if the connected terminals have real-time applications. The other devices can be configured with a "low" priority level (value 3 or 4).

Figure 9.38 illustrates the HTML page, which gives access to the PLC network security configuration parameters (password to access the configuration interface, PLC network ID, password for plant resetting) and the parameters for configuring the priorities of each device on the PLC network, especially the "Default priority" parameter.

The DS2 PLC network can also be configured by using a Telnet console on port 40000 with the following command:

```
C:\>telnet adresseIP_equipement_CPL 40000
```

adresseIP_equipement_CPL is the IP address of the PLC device that we want to configure and that is connected to the configuration PC via the Ethernet interface.

The configuration via the Telnet console gives access to advanced functionalities, such as the PLC device temperature, the notching of some frequency bands, the bridge function, roaming between PLC networks, and so forth.

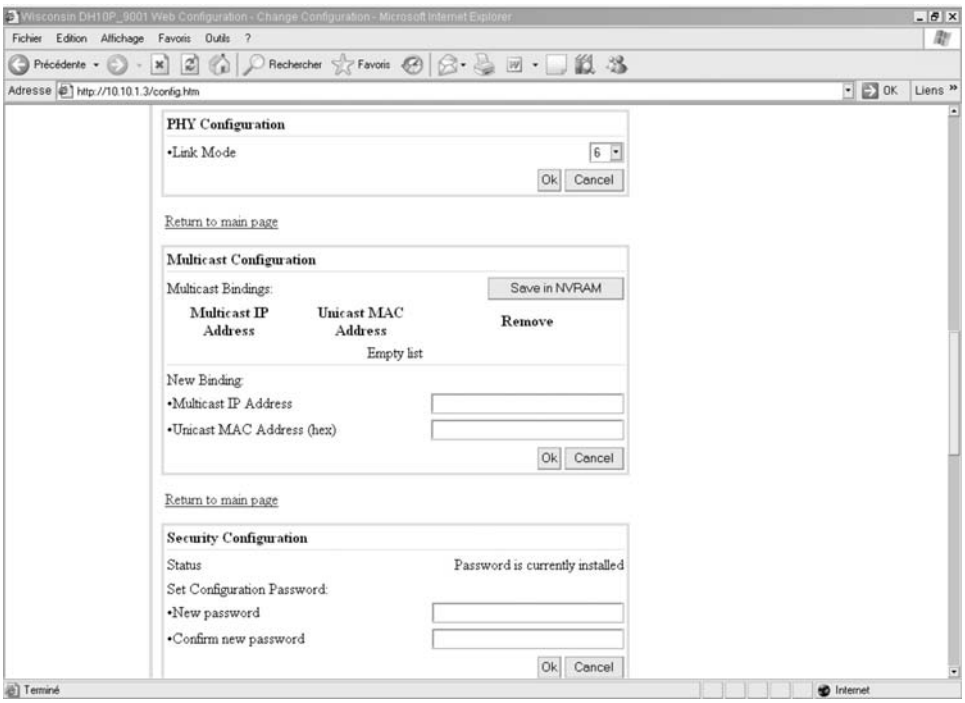

Figure 9.37 Configuration of PHY, multicast, and security parameters for a DS2 PLC device

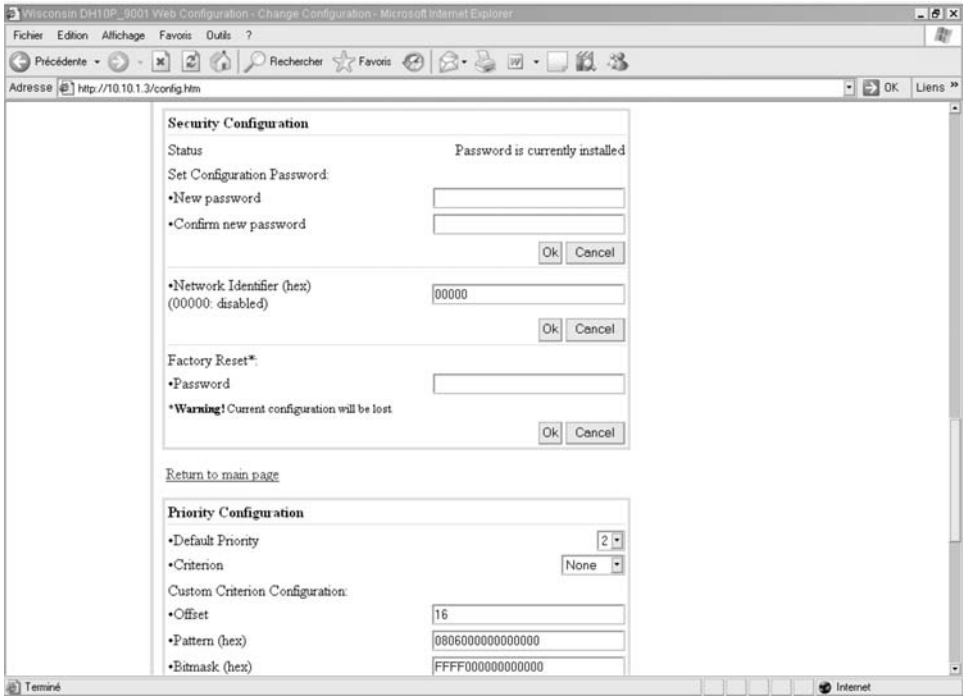

Figure 9.38 Configuration of priority and security parameters for a DS2 PLC device

Configuring Network Parameters

To complete the configuration of a PLC network, it is still necessary to assign the correct network parameters to each device, including the configuration of the IP address, of the subnet mask, of the default gateway address, and of the DNS address.

Before tackling these actual configuration steps, the following sections provide a reminder of a few essential notions on managing network configurations such as IP addresses, subnet mask, and DNS.

Review of Network Parameters

Managing communication in a network is governed by a high number of functionalities related to the standards used. One of them, the Internet Protocol (IP), defines how to communicate with an addressing system and particular routing mechanisms.

IP Addresses

Each computer connected to a local area network or to the Internet uses the combination of two protocols, TCP (or UDP) and IP, better known as TCP/IP or UDP/IP. To communicate, each computer has a single IP address. IP addresses are of the *x.x.x.x* form, where *x* corresponds to a number between 0 and 255.

There are two versions of the IP protocol: IPv4 and IPv6. The IPv4 address, which is most frequently used nowadays, is on 4 bytes and only limited functionalities are available, mainly centered on routing. IPv6 is an evolution of IPv4 which is scarcely implemented in networks. Its address is on 16 bytes, and it includes many functionalities, such as mobility, quality of service, and security management.

Structure of an IPv4 Address

The IPv4 address is on 4 bytes, i.e., 32 bits (1 byte is equivalent to 8 bits).

There are two parts in each IP address:

- The network address;
- A host number corresponding to the address of the computer itself.

Let us imagine a network consisting of three computers, the addresses of which are 145.41.12.1, 145.41.12.2, and 145.41.12.3 respectively. In this case, the network address is 145.41.12.x, 1, 2, and 3 corresponding to the host addresses of the computers.

With such an addressing plan, the network can connect computers with addresses between 145.41.12.1 and 145.41.12.254. 145.41.12.255 is a reserved address, called "broadcast address," which is used for sending information to all the stations of the network. Such an addressing plan offers few possibilities in terms of network connectivity, since it only addresses 254 potential computers.

Depending on the size of the network address, the number of networks and therefore the number of associated hosts can be different. Address classes have been defined to take this difference into account.

Address Classes

In IPv4, five address classes summarized in Table 9.4 have been defined.

These main address classes are defined according to the number of bytes used for the network address:

- For class A addresses, the first byte (8 bits) is reserved for the network address with the first bit set to zero. Thus, the network address is included between

Table 9.4 IPv4 Address Classes

ADDRESS	*ADDRESS RANGES*	*NUMBER OF NETWORKS*	*NUMBER OF HOSTS PER NETWORK*
Class A	1.0.0.0 to 126.0.0.0	126	16,777,214
Class B	128.0.0.0 to 191.255.0.0	16,384	65,534
Class C	192.0.0.0 to 223.255.255.0	2,097,152	254
Class D	224.0.0.0 to 225.0.0.0	Group addresses (multicast)	
Class E	225.0.0.0 to 240.0.0.0	Experimental	

0000000 and 0111111 in the binary format. Knowing that addresses 0.0.0.0. and 127.0.0.0 are reserved, there are therefore $2^7 - 2$, i.e., 126 available class A network addresses, ranging from 1.0.0.0 to 126.0.0.0.

The number of hosts is defined on 3 bytes (24 bits). Since the broadcast address (x.x.x.255) and address x.x.x.0 are reserved, this gives $2^{24} - 2$, i.e., 16,777,214 possible hosts per class A network address.

- For class B addresses, the first 2 bytes (16 bits) are used to define the network address with the first two bits set to 1 and 0. There are therefore $2^{14} - 2$, i.e., 16,384 available class B network addresses, ranging from 128.0.0.0 to 191.255.0.0.

  The number of hosts per network address is defined on 2 bytes. Like for class A addresses, since the broadcast address and address x.x.x.0 are reserved, there are therefore $2^{16} - 2$, i.e., 65,534 possible hosts per class B network address.

- For class C addresses, the first 3 bytes (24 bits) are used with the first three bits set to 1.1 and 0, which gives $2^{21} - 2$, i.e., 2,097,152 available class C network addresses, ranging from 192.0.0.0 to 223.255.255.0.

  The number of hosts is defined on 1 byte (8 bits). Likewise, since the broadcast address and address x.x.x.0 are reserved, there are $2^8 - 2$, i.e., 254 hosts per class C network address.

Class C and D addresses are reserved for experimental multicast addressing.

IP addresses are not automatically allocated, and any address range cannot be allocated to a network. The IANA (Internet Assigned Numbers Agency) is in charge of giving these addresses to any requestor. However, notice that all the available class A and B addresses are already allocated.

IP addresses are routable addresses. This means that they cannot be used for private use.

To avoid improper IP addressing use, the IANA has reserved the three following address ranges for the three main classes for strictly private use:

- Class A: 10.0.0.1 to 10.255.255.254
- Class B: 172.16.0.1 to 172.63.255.254
- Class C: 192.168.0.0 to 192.168.255.254

To connect to a network with a different addressing plan or to the Internet, each station having a private IP address must specify a default gateway address. This address corresponds to a station dealing with network routing and is used both for sending and receiving requests from a nonroutable environment (private network) to a routable environment (Internet).

In the case of Internet connection sharing via a gateway, the gateway is in charge of sending requests from a private (therefore nonroutable) environment to the Internet (routable) environment. In this case, the default gateway address is the gateway IP address.

Subnet Mask

The mask is used for knowing the network address of a computer via a binary subtraction between the mask and the computer IP address.

If the IP address of a computer is 192.168.0.1 and if the 255.255.255.0 mask is applied to it, the binary subtraction of these two addresses gives 192.0.0.0, i.e., the network address.

In general, the masks for class A, class B, and class C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

During mask configuration for two computers, if the IP address of one of them is 192.168.1.1 with the 255.255.255.0 mask and if the IP address of the second one is 192.168.1.10 with the 255.225.0.0 mask, their network addresses (192.168.0.x and 192.168.1.x) are not identical. Therefore, they do not belong to the same network and cannot communicate.

DNS (Domain Name Service)

DNS is a hierarchical structure consisting of a group of servers used for associating an IP address with a domain name consisting of an organization name (e.g., Google) and a classification (.fr, .com, and so forth).

In this way, it is much easier to remember Web site, messaging, or FTP addresses rather than their associated IP address.

It is still possible to know the IP address of a particular server or of a Web site. For example, the IP address of the www.google.com Web site can be found out just by ping-ing to this site as illustrated in Figure 9.39.

In general, two DNS server addresses are requested when the network parameters are configured in order to allow access to the network, should a server be defective. DNS addresses are necessarily IP addresses.

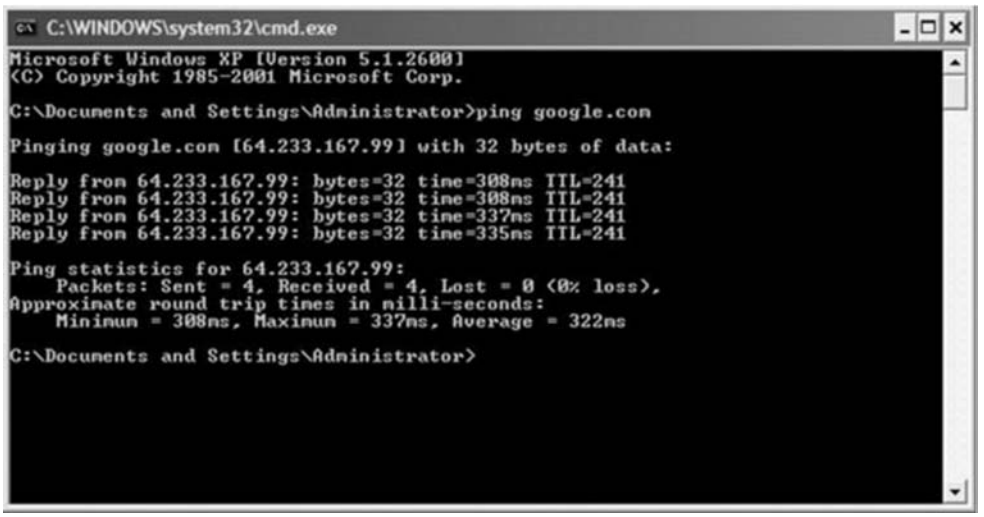
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping google.com
Pinging google.com [64.233.167.99] with 32 bytes of data:
Reply from 64.233.167.99: bytes=32 time=308ms TTL=241
Reply from 64.233.167.99: bytes=32 time=308ms TTL=241
Reply from 64.233.167.99: bytes=32 time=337ms TTL=241
Reply from 64.233.167.99: bytes=32 time=335ms TTL=241
Ping statistics for 64.233.167.99:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimun = 308ms, Maximun = 337ms, Average = 322ms
C:\Documents and Settings\Administrator>

Figure 9.39 IP address of www.google.com

Configuring Network Parameters Under Windows XP

In the Configuration panel, select "Network" then, in the network components area, choose the TCP/IP component of your Wi-Fi board and click on "Properties" to open the dialogue box.

Fill in the various fields using information given by your Internet service provider if this is necessary:

- IP address corresponding to the computer IP address;
- Subnet mask used for knowing the network address and the subnet address of the IP address above;
- Default gateway corresponding to the address of the network computer connected to the Internet;
- DNS addresses generally given by the IAP or the network administrator.

For Windows versions other than Windows 2000 and XP, the computer must be rebooted.

In the case of Windows 2000 or XP, the activation of the user-defined network parameters can take up to ten seconds.

Configuring Network Parameters Under Linux/BSD

To configure the IP address and the subnet mask of the board, enter in a shell:

```
# ifconfig eth0 10.0.0.2 netmask 255.255.255.0
```

To configure the gateway address (10.0.0.1 in this case), enter:

```
# route add default gw 10.0.0.1
```

The route command is used for checking whether the gateway address was actually added into the routing table:

```
# route
Kernel IP Routing Table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface
Default         10.0.0.1        0.0.0.0         UG    0      0
0 eth0
```

To configure the address of the name server or servers (DNS), just print out the resolv.conf file that is in the /etc directory using the vi command:

```
# vi/etc/resolv.conf
```

Here is an example for the resolv.conf file:

```
nameserver adresse_IP_DNS
domain nom_de_domaine
```

nameserver is used for defining the primary DNS address, whereas domain defines the network domain name, if it has a domain. The domain name is given by

the IAP like DNS addresses. If there are several DNS addresses, just add a line with nameserver adress_IP_DNS for each additional DNS address.

This configuration can also be done semiautomatically by configuring the /etc/pcmcia/network.opts file in case the network interface card is a PCMCIA board or the /etc/network/interfaces file for a PCI or Mini-PCI board.

CHAPTER 10

PLC in the Home

In spite of the still relatively high cost of PLC devices, more and more people are tempted to install a power line communication home network. The fact that no cables have to be laid seems to be the decisive factor for such a choice.

The installation of a PLC network in a house or apartment is actually extremely simple. All you have to do is connect the PLC devices to the electrical network and configure them. Ideally, you should have an Internet connection via an ADSL modem (cable, satellite, or even 56K) that you just have to connect to a PLC device acting as a gateway to provide Internet access to all the electrical network outlets.

New Internet access offers are made available by providers via two boxes: an ADSL modem, which connects to the voice jack, and a video decoder box, which receives the Internet IP video stream and broadcasts it to a TV set or an HDTV screen. Some Internet access providers (IAP) add two PLC devices to these boxes in order to connect them. This tendency will intensify with the development of HD (high definition) video over IP services for domestic customers, which will be used for broadcasting video streams to the various TV screens in the house. PLCs are one of the best solutions for broadcasting these IP streams in terms of throughput or signal coverage area.

The topology of a PLC home network may vary depending on requirements and electrical network architectures as well as the chosen devices and the network operating mode used.

Figure 10.1 illustrates a PLC home network in which the PLC device is connected to the Internet by means of a modem enabling connection sharing.

This chapter is devoted to the optimum installation of a PLC home network, from the choice of a device to its installation and its configuration. The installation of a home network is not a very difficult job, but it requires compliance with some rules, notably concerning the electrical network and safety measures.

Electrical Security

PLC technology uses the 110-220V/50 to 60 Hz LV electrical network as a communication medium. Since this network is hazardous for human safety, it is important to comply with a few elementary safety measures in order to avoid electrocution risks.

Figure 10.2 illustrates a typical sign symbolizing electrical hazards.

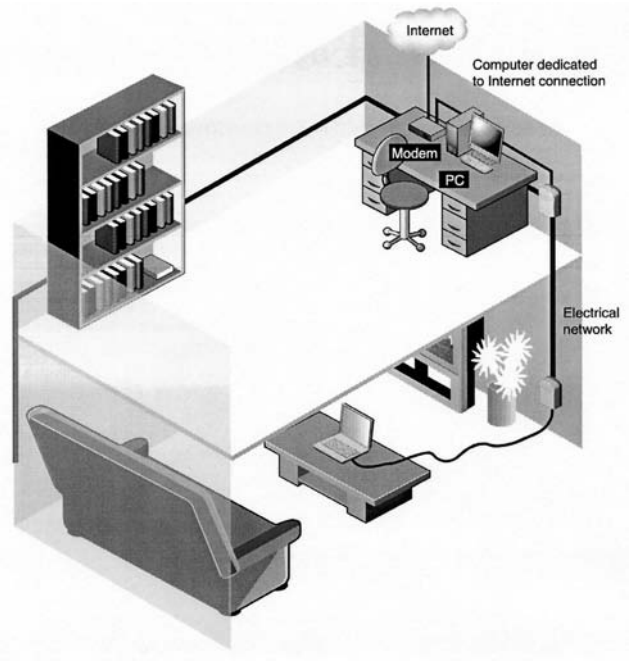

Figure 10.1 PLC home network with shared Internet connection

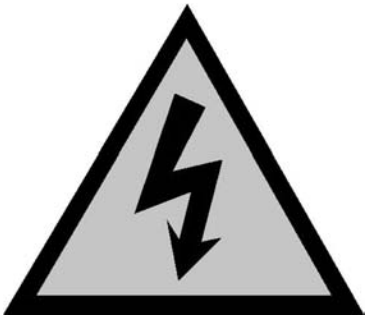

Figure 10.2 Sign symbolizing an electrical hazard

The main electrical safety rules to be complied with are the following:

- Install a 500 mA differential circuit breaker for protection against short circuits.
- Protect outlets using a circuit breaker or a fuse not exceeding 16A.
- Do not expose the devices to sun or heat.
- Do not clean the devices using detergents or aerosols.
- Do not disassemble the devices without having disconnected them and waited for the discharge of the electronic components for a few minutes.
- Do not install devices close to water inlets (bathtub, shower, washer, washbasin, swimming pool, and so forth).

- Do not overload power strips or extension cords in order not to increase electrocution or fire risk.
- Comply with the operating instructions of the PLC devices.
- Do not try to install PLC injector systems on electrical wirings without the help of a competent electrician.

If in doubt concerning any of these rules or the condition of the electrical network on which you wish to install the PLC network, it is recommended that you contact a professional electrician or a PLC specialist.

Choosing a PLC Technology

As we saw in the previous chapters, there are several PLC technologies and specifications insofar as the IEEE 1901 standard is not available yet. Even though they share some functionalities, these specifications have different characteristics. Only the HomePlug consortium appears as a de facto PLC standard, since most devices available on the market comply with this specification.

Table 10.1 summarizes criteria for the selection of the various PLC technologies currently available.

Choosing Equipment

The prices of HomePlug 1.0 products have fallen drastically since the emergence of HomePlug Turbo products, offering throughputs in keeping with current application requirements. The emergence of HomePlug AV devices has in turn resulted in falling HomePlug 1.0 and Turbo device prices.

For the requirements of current applications (broadcasting of IPTV, data and voice Internet flows in the house), HomePlug AV devices seem to coincide with the best throughput/budget ratio expected from domestic users.

Increasing network application throughput requests between terminals of a domestic installation (network games, broadcasting of data flows, voice and video between media hubs and receiving or display stations) or to receive the services

Table 10.1 PLC Technology Choice Elements

PLC TECHNOLOGY		*PREFERRED USE AND FIELD OF APPLICATION*
HomePlug	1.0, Turbo, AV	Home networks, Internet broadcasting, IP video streams (HomePlug AV), audio broadcasting
	Oxance	Professional networks, industrial applications, improved service quality
	BPL	PLC for the MV (medium voltage) electrical networks of local authorities
DS2		Professional networks, high rate home networks (voice, data, high definition IP video)
Spidcom		Professional networks, industrial applications, automotive PLC
Main.net		PLC for the electrical networks of local authorities

offered by Internet access providers from anywhere in an installation, requires devices with a throughput around 200 Mbit/s at the physical layer level, which is the case of HomePlug AV devices.

Insofar as all HomePlug devices are compatible between themselves for 1.0 and Turbo, various HomePlug products suited for the following uses will nonetheless coexist for some time.

- *HomePlug 1.0:* Web navigation, electronic mail;
- *HomePlug Turbo:* Internet, IP telephony, data (exchange of bulky files), images (IPTV or MPEG-2 or MPEG-4 video on demand);
- *HomePlug AV:* digital HD video in the IP format (high-definition MPEG-2, for example) broadcast to several display stations.

Placing Devices on the Electrical Network

To achieve a network quality and performance enabling the broadcasting of Internet flows (voice, data, IPRV), it is important to place the PLC devices as efficiently as possible on the electrical network according to the following criteria:

- Topology of the installation's electrical network;
- Place of IP terminals and PC supposedly connected to the flows coming from the Internet modem.

The following place is ideal for PLC devices:

- Close to the circuit breaker panel from which the various electrical wirings supplying the outlets, electrical devices, and the lights of the house start.
- Close to the Internet modem connected to the public STN (switched telecommunications network) on the voice jack.

Figure 10.3 illustrates a regular domestic installation wiring diagram with Internet access. The PLC devices are placed on the outlets located close to the voice jack connecting the house to the Internet.

In such an installation, three PLC devices can be used for receiving the Internet flow with a satisfactory coverage:

- A gateway PLC device connected to the Ethernet jack of the Internet modem and to outlet 1;
- A PLC device for fixed PC (outlet 3) which can be on the same electrical wiring;
- A PLC device for portable PC (outlet 5 or 6), which can be placed on a different floor to provide domestic installation mobility.

This network configuration with three devices is the most widespread in a domestic environment. An increasing number of homes are equipped with at least two computers and a high speed Internet connection of the InternetBox type.

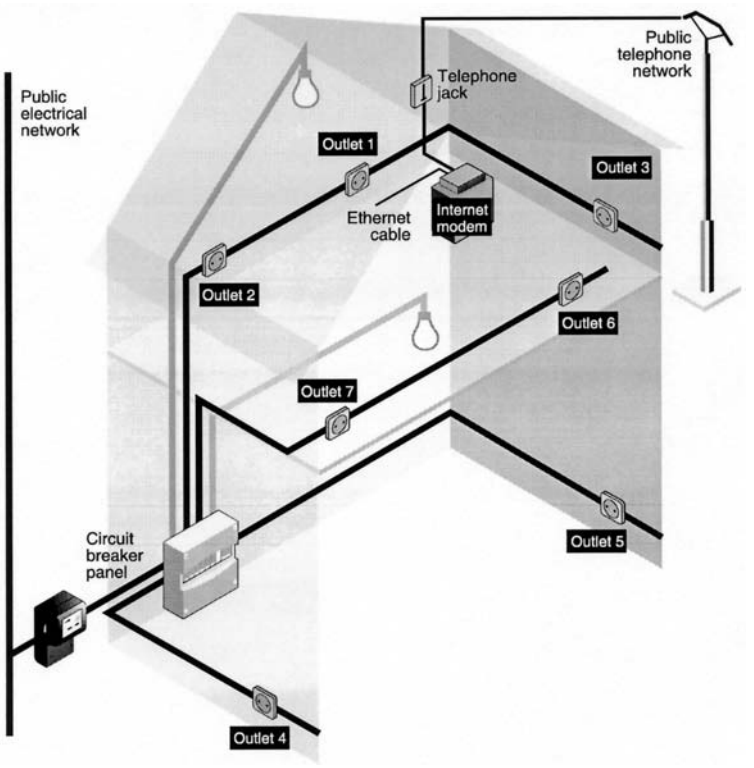

Figure 10.3 Regular wiring diagram for a domestic installation with Internet access

Figure 10.4 illustrates the same home network with all the devices installed for the broadcasting of the various Internet flows to the outlets of the electrical network.

The PLC device located on outlet 3 is used by the computer for connecting to the Internet via the outlets (outlet 3 to outlet 1). Therefore, it is important to find a satisfactory compromise between the desired throughput, the position of the PC in the house, and the quality of the PLC communication links between outlet 3 and outlet 1.

With HomePlug Turbo devices, an outlet with a throughput between 12 Mbit/s and 75 Mbit/s should be found using PLC configuration tools (such as the Intellon Power Packet Utility described in Chapter 9), which is generally the case of outlets located on the same floor in adjacent rooms.

The PLC device located on outlet 5 is used by the TV decoder for connecting to the InternetBox via the electrical network and recovering the video streams from the Internet connection. These video streams require a minimum stable 1-Mbit/s useful throughput for fluid TV display. It is important not to degrade the video signal too much on the electrical network so as not to lose images. This constraint supposes that the PLC communication link between outlet 5 and outlet 1 provides a 1.5-Mbit/s useful throughput. This throughput can be checked using a PLC configuration tool. The involved device must be connected directly to a wall outlet or a biplite, but not to a power strip.

Table 10.2 lists, for a HomePlug Turbo device, the correspondences between the throughputs displayed by the configuration tool and the useful throughputs

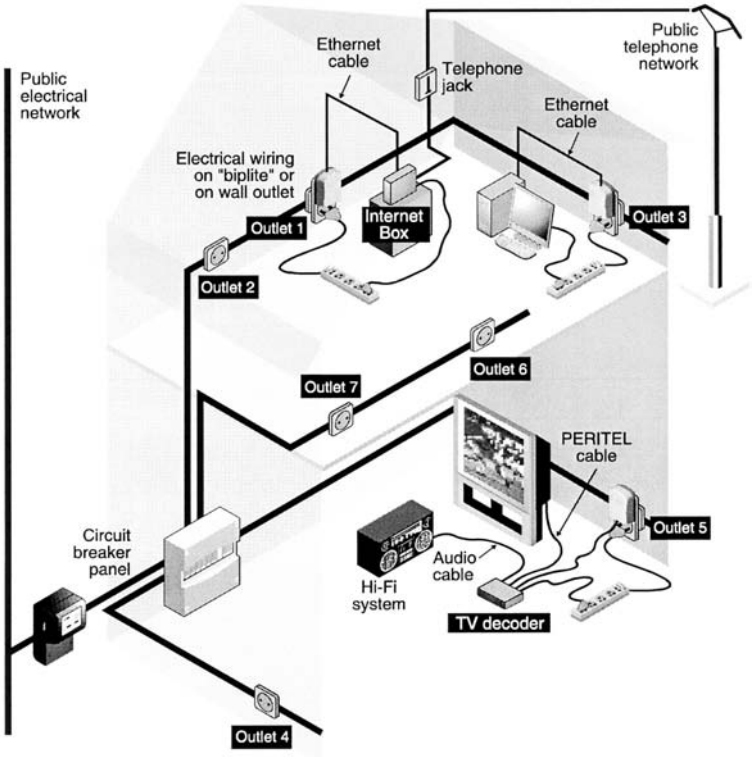

Figure 10.4 Place of PLC devices in the domestic installation

available for the IP network applications based on the PLC network. According to this table, it is important to find an outlet 5 that gives a minimum 10-Mbit/s displayed throughput.

The analog telephony flow originating from the Internet connection and available on the RJ-11 connector of the InternetBox connected to the telephone jack can also be broadcast over the electrical network.

Wingoline PLC devices from Niroda, for example, operate in the 3.3- to 8.2-MHz frequency band according to a proprietary communication protocol different from that of HomePlug devices. The PLC network created with Niroda devices is therefore not interoperable with a HomePlug PLC network. Up to 24 Niroda PLC devices can be placed on the same electrical network for adding analog telephone lines.

Figure 10.5 illustrates the possible connectivities from the InternetBox provided by the IAP with the following PLC networks:

- HomePlug Ethernet PLC network used for connecting the IP terminals of the house to the InternetBox Ethernet jacks;
- RJ-11 PLC network used for connecting analog telephone devices to the InternetBox voice jack;
- RJ-11 PLC network used for connecting the InternetBox to the France Télécom voice jack via the house electrical network.

Table 10.2 Displayed and Useful HomePlug Turbo PLC Throughputs

DISPLAYED THROUGHPUT (Mbit/s)	*USEFUL THROUGHPUT (Mbit/s)*
85	12.5
75	11.8
55	9.42
45	8.79
35	8.23
25	7
14	4.5
12.83	3.5
11	3.2
10.16	2.9
8.36	2.4
6.35	2
4.04	1.22
3	0.89
1	0.33
0.9 (ROBO mode)	0.2

The following Niroda devices of the RJ-11 PLC network can be placed as indicated in Figure 10.6:

- InternetBox connected to the electrical network to outlet 1 via its RJ-11 telephone plug;
- Telephone 1 connected to outlet 6 by means of a Niroda device to the telephone PLC network;
- Telephone 2 connected to outlet 5 in the same manner.

Since the throughputs required for telephony are on the order of 20 Kbit/s, it is quite realistic to envisage this on the electrical installation of a medium-sized house (three or four rooms).

Figure 10.7 illustrates the following signals or flows circulating over the electrical and telephone networks of the domestic installation:

- Analog telephone signal between the telephone sets and the InternetBox RJ11 connectors;
- IP data flow originating from the ADSL Internet connection.

Configuring Security Parameters

Even within the household, the protection of a PLC network represents a major step. The use of electrical wiring implies that the network beams a more or less wide

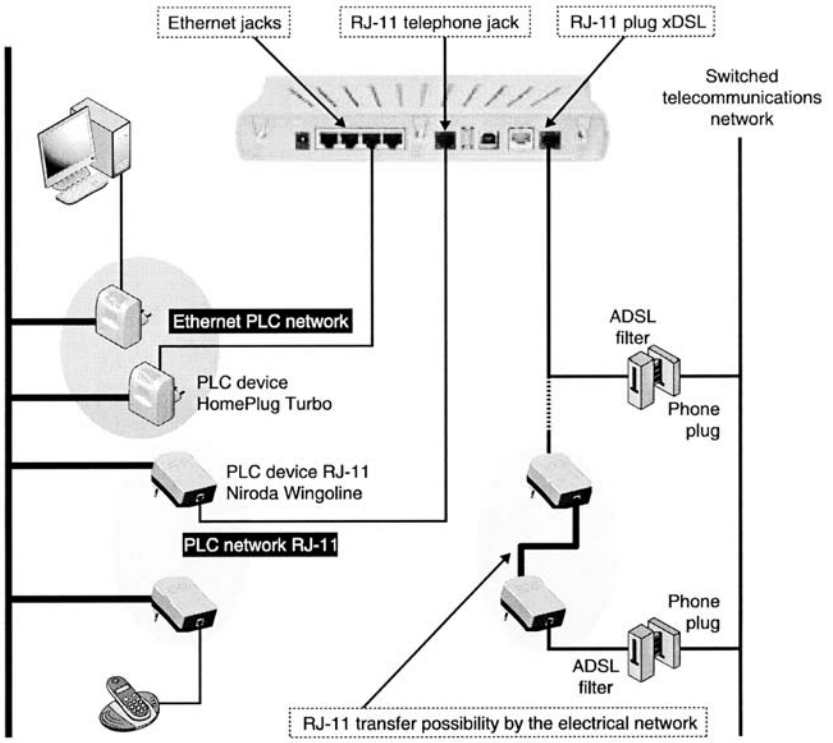

Figure 10.5 Various PLC networks connected to an InternetBox

coverage area that can extend beyond the home area. This allows anybody to access the network and to use its Internet connection, for example.

PLC networks provide security mechanisms likely to prevent eavesdropping with a suitable password management scheme.

To protect the network in a still more reliable way, there are other firewall-based solutions (authentication server and virtual private network).

Configuring the PLC Gateway

The gateway concept may seem ambiguous since there are potentially several gateways in the same network determined by the following elements:

- The Internet, modem, or InternetBox gateway used for connecting the house to the Internet network, generally by means of the telephone jack with an xDSL connection;
- The Ethernet gateway used for connecting the modem, a router, or the InternetBox to the local area network and for configuring the security parameters detailed in the following sections;
- The PLC gateway used for connecting the Internet gateway to the electrical network and for broadcasting IP flows from the Internet in the entire network.

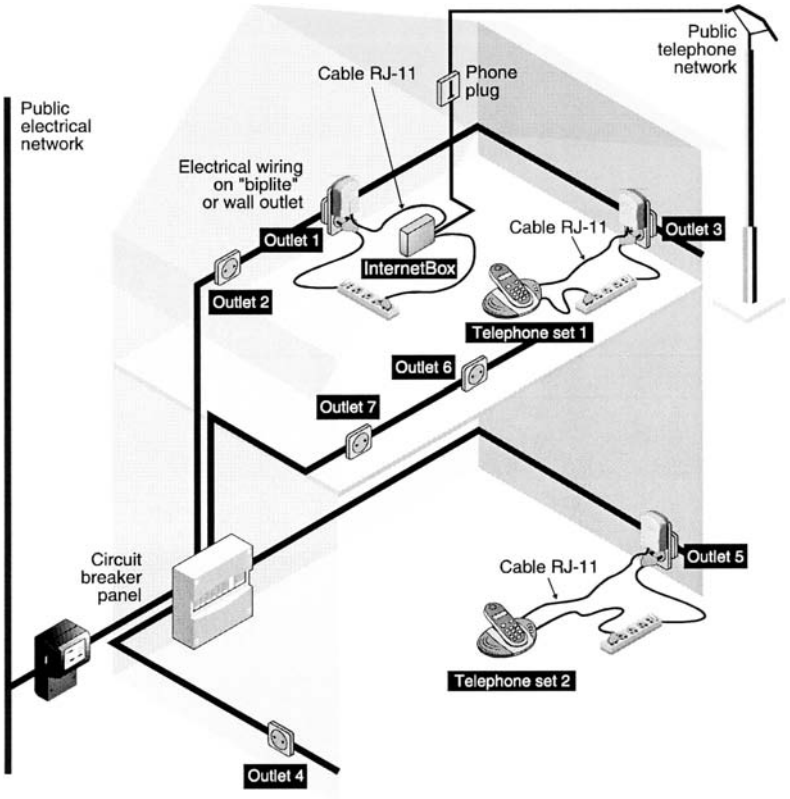

Figure 10.6 Place of devices used for broadcasting IP telephony over the electrical home network

Figure 10.8 illustrates the location of these various gateway types in a domestic installation.

For a HomePlug device, the PLC gateway requires no specific configuration compared to the other PLC devices of the network since HomePlug Turbo operates in peer-to-peer mode. The specific nature of the PLC gateway results from the fact that this device is connected to the Internet gateway and that all the outgoing IP flows to the Internet go through this device.

The only HomePlug parameter to be specifically configured on the PLC gateway is the priority (CA0, CA1, CA2, and CA3 parameters specifying four priority levels). Table 10.3 summarizes the characteristics of these priority levels for HomePlug.

These eight priority classes are inherited from the description of the IEEE 802.1D standard classes by simplifying the eight 802.1D classes in four PLC classes.

To configure the values of CA priority parameters on the PLC gateway, simply set the value to CA3 to allow prioritization of the incoming and outgoing traffic of the PLC device that can be the bottleneck of the PLC network.

Insofar as the PLC configuration tools cannot be used for configuring this parameter, I have developed a specific tool for the Windows operating system that starts as an executable file. This program is available at the following address: http://carcelle.fu8.com/ConfigurationPrioriteCPL.zip.

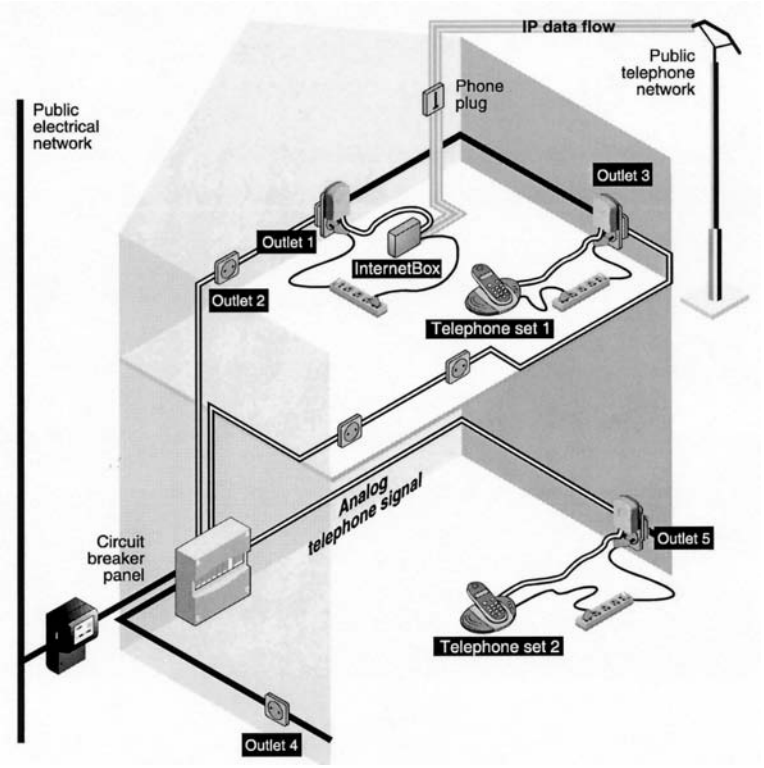

Figure 10.7 Broadcasting of the analog telephone signal over the electrical home network

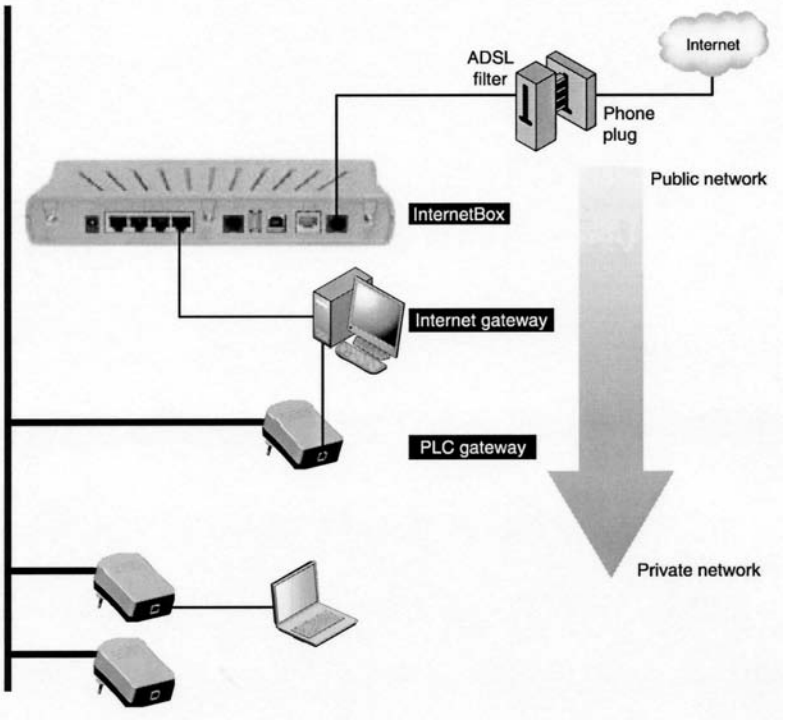

Figure 10.8 Location of the various gateways from the public network to the private network

Table 10.3 Data Traffic Priority Levels for the PLC Gateway

PRIORITY FOR DATA TRAFFIC	*HomePlug 1.0 AND TURBO PRIORITY*	
0	CA0	Low priority
1		
2	CA1	
3		
4	CA2	High priority
5		
6	CA3	
7 (highest priority level)		

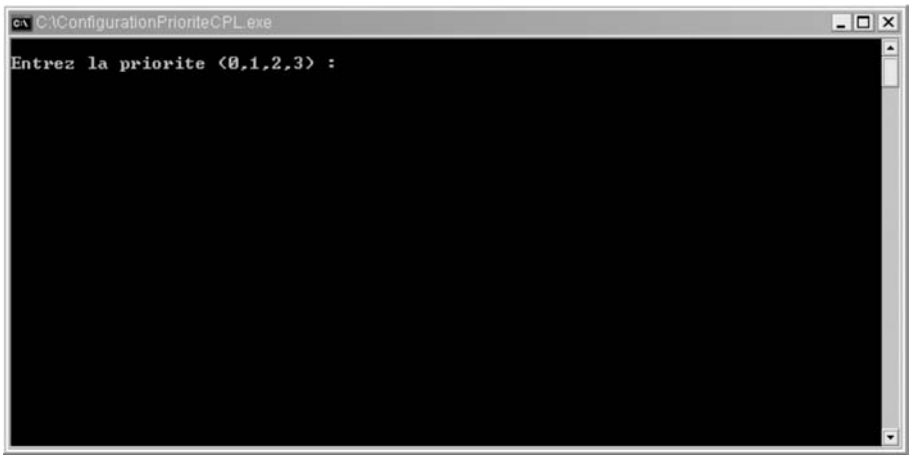

Figure 10.9 Launching the PLC priority configuration tool

The WinPCap tool used for managing inputs/outputs on the network interface card must be installed beforehand. This tool is generally pre-installed by the PLC configuration tools. If not, it can be downloaded at the following address: http://www.winpcap.org/install/bin/WinPcap_3_1.exe.

Once the WinPCap tool is downloaded and installed, just proceed in the following way to install the ConfigurationPrioritéCPL tool:

- Download the ConfigurationPrioritéCPL.zip file, then decompress it in a local directory.
- Run the tool by double-clicking on the ConfigurationPrioritéCPL.exe file.

Once the tool has been launched, a DOS window prompts you to choose one of the priorities, 0(CA0), 1(CA1), 2(CA2) or 3(CA3), as illustrated by Figure 10.9.

Once the priority is chosen, the tool prompts you to choose the Ethernet network interface card of the PC locally connected to the PLC device. The IP address information is used for recognizing the correct network interface card. In the case of Figure 10.10, the board connected to the PLC gateway is board 3 whose IP address is 192.168.0.10.

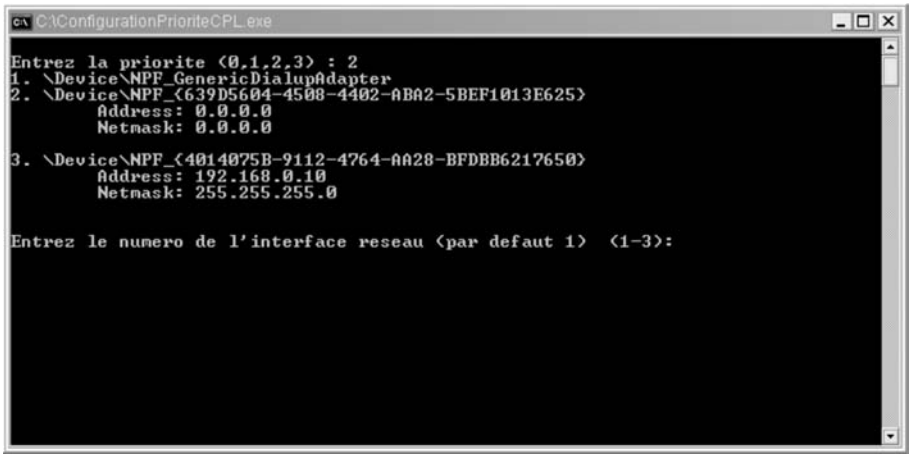

Figure 10.10 Configuring the Ethernet board connected to the PLC device

Once the network interface card has been chosen, the DOS window closes; this indicates that the priority configuration is completed.

It is important to identify the PLC device with the highest priority level and to maintain its connection to the Internet gateway or to the InternetBox.

Configuring PLC Security

The configuration of PLC security is a major aspect of the PLC network implementation enabling the securing of data exchanges between the electrical network PLC devices. Since the PLC signal propagates beyond the house meter boundaries, any malevolent person can intercept the data if the PLC devices are simply configured using the default parameters of the NEK.

Several PLC networks can also be installed on the same electrical network with security configuration by configuring various NEK on the connected HomePlug devices.

As we saw in Chapter 9, dedicated to the configuration of HomePlug PLC devices, the NEK key must be configured on all the PLC devices to be installed using configuration tools such as Power Packet Utility from Intellon for HomePlug 1.0/Turbo and Power Manager from AsokaUSA for HomePlug AV.

This tool (available at the following address: http://asokausa.com/downloads/Power Manager1.2.0-Common.zip is used for configuring the NEK on the various PLC devices. In order to do this, simply connect the PLC devices one by one to the PC on which the configuration tool is installed by means of a network cable (Ethernet or USB depending on the PLC device model).

Once the device is connected to the PC, the configuration tool runs via the "Start" menu. The window illustrated in Figure 10.11 then opens. The device locally connected to the PC is described in the "Devices" window pane.

The "New Network Password" field is used for modifying the network key set by default to the HomePlug value and for assigning a specific value to it for the domestic installation network.

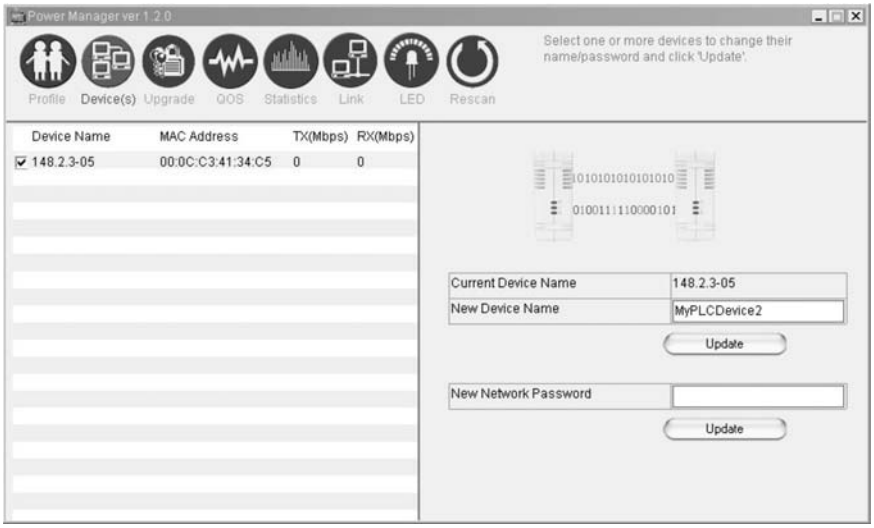

Figure 10.11 "Products" tab of the AsokaUSA PLC configuration tool

This key must have between 4 and 24 characters and include numerals and (lowercase and uppercase) letters if possible, for example, PLCNetworks. Just click on "Update" for local device configuration. The configuration is confirmed thanks to a window indicating "Network Encryption is successfully changed" as illustrated in Figure 10.12.

To perform the same operation on all PLC devices, simply connect them to the configuration PC.

Once all the PLC devices are correctly configured, the "Devices" tab is used for ensuring that all the PLC devices can be seen from the PLC gateway.

Figure 10.13 illustrates a PLC network with two PLC devices and the following PLC links:

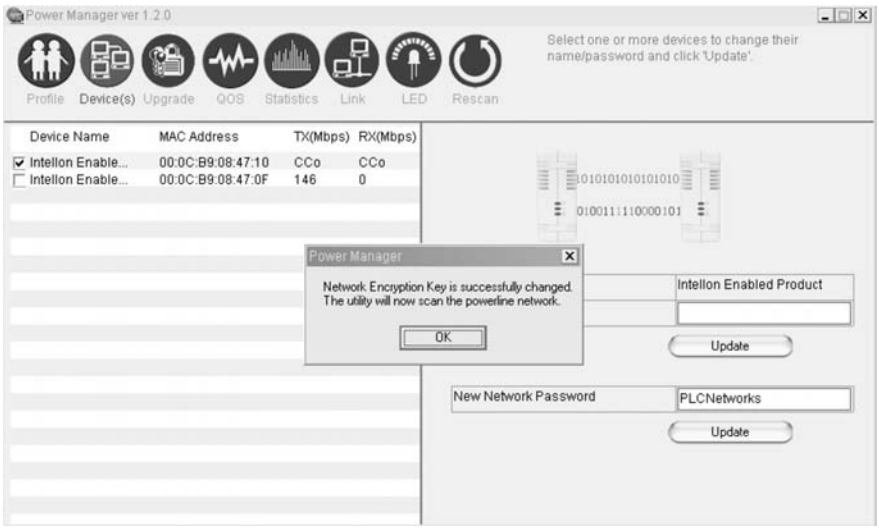

Figure 10.12 NEK configuration in "Security" tab

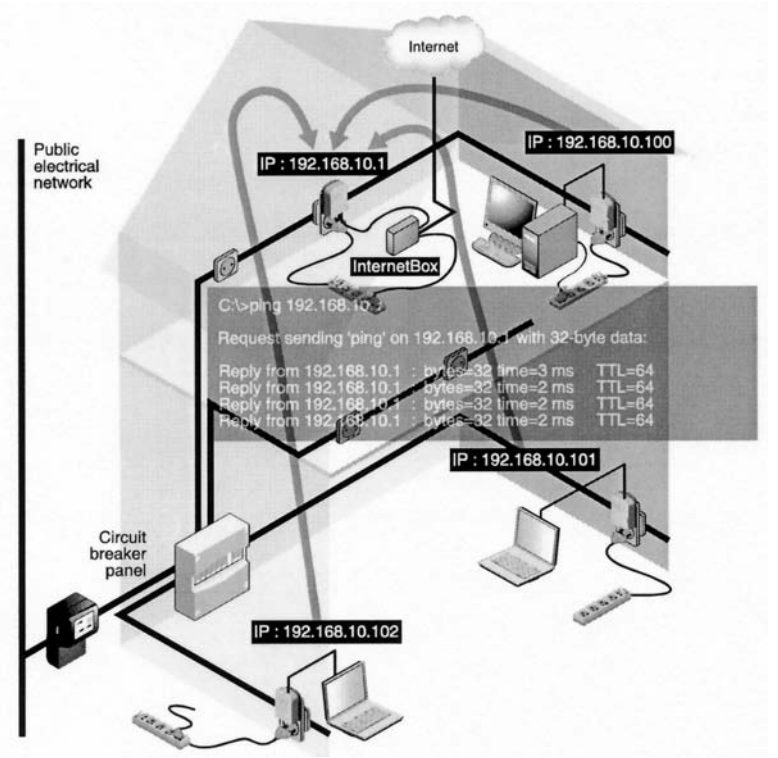
Internet
Public electrical network
IP : 192.168.10.1
IP : 192.168.10.100
InternetBox
C:\>ping 192.168.10.1
Request sending 'ping' on 192.168.10.1 with 32-byte data:
Reply from 192.168.10.1 : bytes=32 time=3 ms TTL=64
Reply from 192.168.10.1 : bytes=32 time=2 ms TTL=64
Reply from 192.168.10.1 : bytes=32 time=2 ms TTL=64
Reply from 192.168.10.1 : bytes=32 time=2 ms TTL=64
IP : 192.168.10.101
Circuit breaker panel
IP : 192.168.10.102

Figure 10.13 Testing good operation of the PLC network at the IP level

- MAC device = 00:0C:B9:08:47:0F to living room device: "good" quality with 24.55 Mbit/s displayed throughput;
- MAC device = 00:0C:B9:08:47:10 to bedroom device (HomePlug 1.0): "first-rate" quality with 13.43 Mbit/s displayed throughput.

Since the PLC network security is confirmed, the security of the terminals themselves can be configured.

Maximum Number of PLC Devices on the Same Network

The HomePlug 1.0 and Turbo specifications indicate that a PLC network with the same network key can have a maximum of 15 devices. Since several NEK cannot be configured with HomePlug 1.0 and Turbo devices, a device can belong to only one PLC network at a time. This problem is solved with the HomePlug AV standard that enables various network configurations and several network keys for the same device.

Testing Operation of the PLC Network

Once the various PLC devices of the network are configured, it is recommended that you check the good operation of the domestic installation network links by performing a test with the PLC configuration tool ("Products" tab).

To test the good operation of the PLC network, it can also be useful to run "Ping" commands from the PC connected to the PLC network to the InternetBox as illustrated in Figure 10.13.

For this purpose, all the PCs or terminals must be in the same addressing plane as the InternetBox (for example, for an IP network of the 192.168.10.x type, the InternetBox is in IP = 192.168.10.1 and the other devices in IP = 192.168.10.100, 101, 102, and so forth). The configuration of the network address (or IP) for a PC is detailed in Chapter 9.

To start the "Ping" command, just proceed as follows:

- Click on "Start" then on "Execute."
- Enter cmd. A DOS window opens.
- Enter the following command:

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data :

Reply of 192.168.10.1 : bytes=32 time=3 ms TTL=64
Reply of 192.168.10.1 : bytes=32 time=2 ms TTL=64
Reply of 192.168.10.1 : bytes=32 time=2 ms TTL=64
Reply of 192.168.10.1 : bytes=32 time=2 ms TTL=64
```

If replies are sent back with this command, this means that the network links are configured and ready to be used by applications.

Firewall

The connection to the Internet network can provide access to the home network to ill-intentioned people. The only solution to prevent these attacks consists of using a firewall. The purpose of a firewall is to authorize certain protocols only, within the home network, depending on the port number used.

Each protocol uses a specific port number (e.g., port 80 for HTTP [hypertext transfer protocol] which enables it to be recognized as such by the network). By only authorizing certain ports and therefore certain applications, such as electronic mail, HTTP, or FTP, all the other ports are prohibited.

Among the many firewalls available on the market, there are free ones such as those available in Linux distributions using a 2.4 or 2.6 kernel.

Windows XP enables you to establish software firewalling rules for a station's network connection but not for the entire network, unlike hardware firewalls, which can prohibit a protocol for an entire network.

To access the Windows XP software firewall, just proceed as follows:

In the Configuration panel, select "Network connection" to display the window illustrated in Figure 10.14.

Select "Ethernet network connection" to display the dialogue box illustrated in Figure 10.15.

Click on the "Advanced" tab and click on "Settings" to display the Windows Firewall dialog box as illustrated in Figure 10.16.

In the "General" tab, tick the "On" box (recommended).

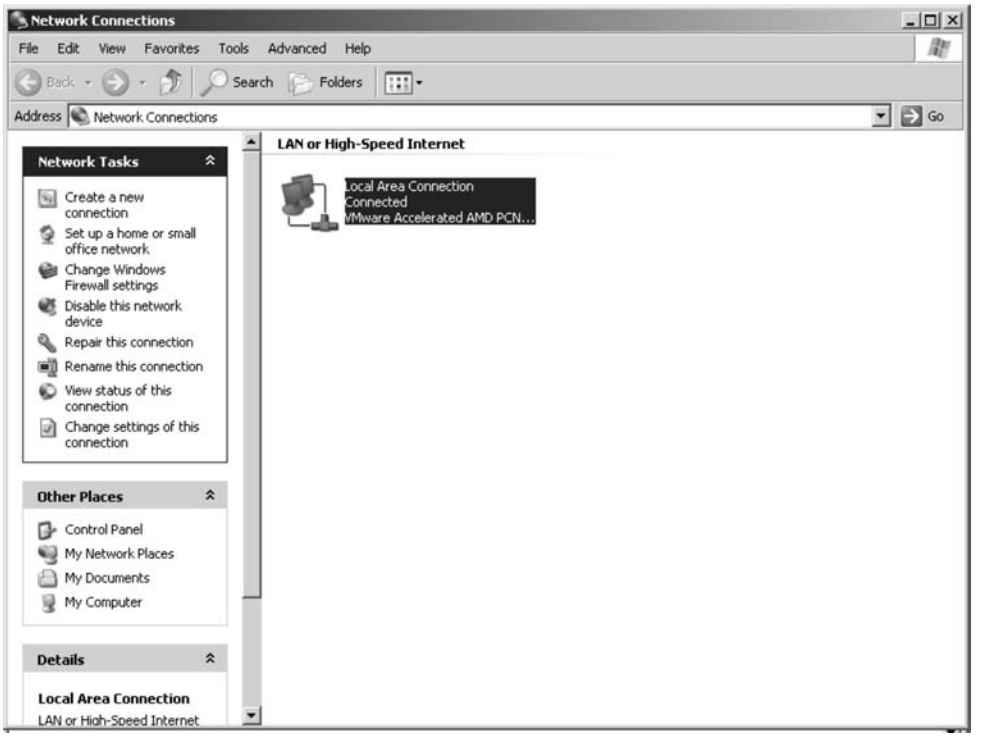

Figure 10.14 Windows XP network connection window

Hardware firewalls must be installed on the computer connected to the Internet. This is ideally a dedicated computer, such as the access gateway defined above (see Figure 10.17).

VPN and PPPoE

The only way of guaranteeing the total security of a PLC network consists of using a VPN (virtual private network) as explained in Chapter 4.

The use of an authentication server is only necessary if the network requires a high level of protection. The authentication scheme is used, as its name implies, for reliably authenticating any user who wants to connect to the network. RADIUS (remote authentication dial-in user server of which a free version called "Freeradius," is available at the following address: http://www.freeradius.org, is the most widespread authentication protocol).

To protect a network on an even higher reliability level, a VPN is essential. VPNs are used for fully protecting PLC network links by means of authentication and encryption mechanisms. At present, IPsec is the most widespread protocol in VPN. However, the use of an IPsec VPN requires rather powerful computers. It also requires the client computers to have the configuration required by their VPN client.

Using authentication servers or VPN servers requires the adding of the corresponding functionalities coinciding with the level of a specific gateway in case the gateway for accessing the Internet already incorporates a DHCP server and an NAT router, as illustrated in Figure 10.18.

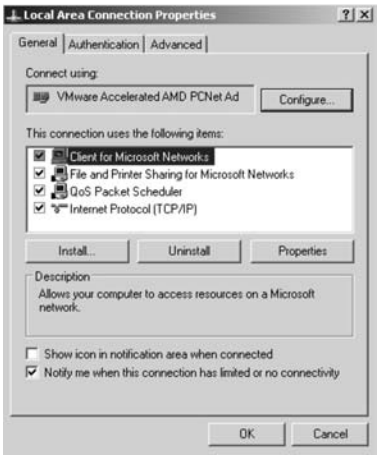

Figure 10.15 Ethernet properties dialogue box

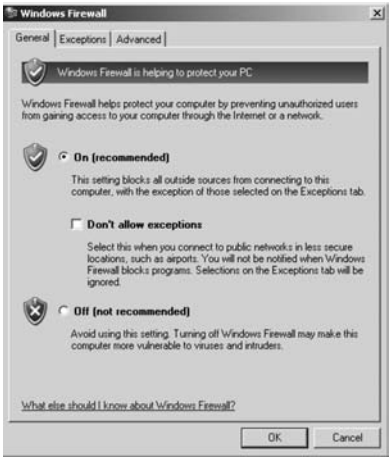
Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
What else should I know about Windows Firewall?
OK
Cancel

Figure 10.16 Advanced connection firewall configuration parameters

Another way of improving the security of the PLC network and of the IP local area network consists of installing a PPPoE server and an associated RADIUS server. This technique is used for implementing IP "tunnels" between the computers connected to the PLC local area network and to the Internet gateway; these clients are authenticated on the RADIUS server.

If an intruder successfully connects to a PLC local area network, he cannot use the local area network as long as he is not connected to the PPPoE server and to the RADIUS server on the gateway. Therefore, the hacker's station can neither access other computers connected to the PLC network nor access the Internet via the PLC network gateway.

Figure 10.19 illustrates the concept of PPPoE tunnels established between the client computers and the Internet gateway and enabling the securing of exchanges between the gateway (and the Internet) and these client computers.

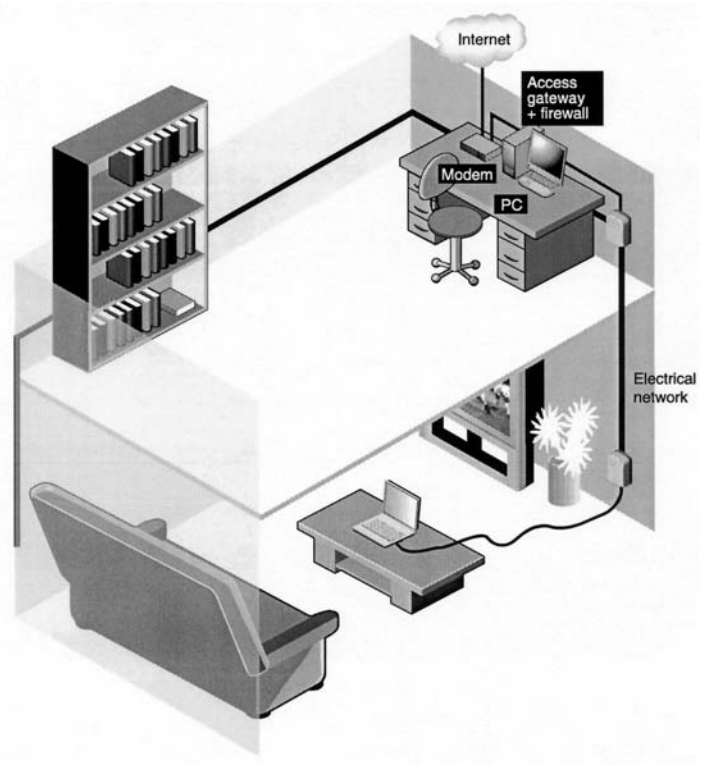

Figure 10.17 PLC network with access gateway protected by a firewall

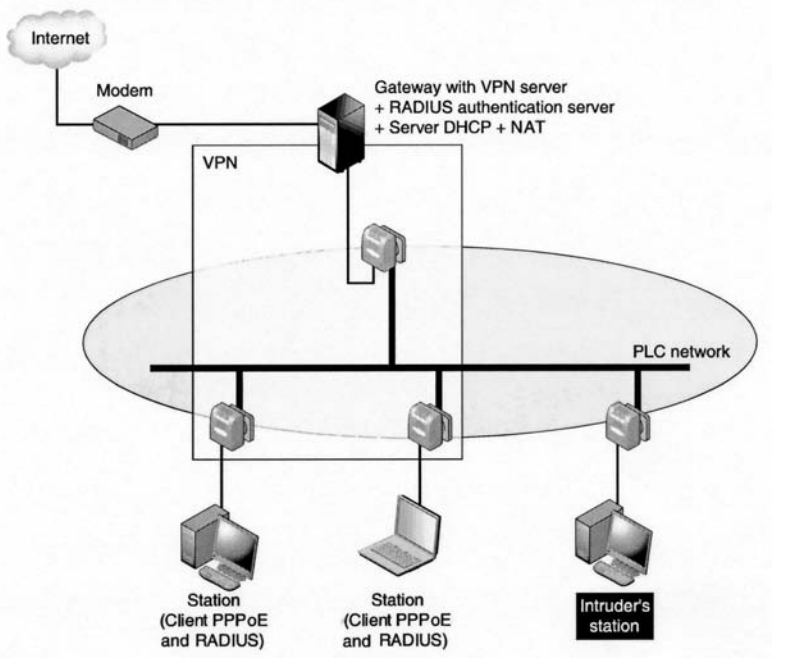

Figure 10.18 PLC network with gateway protected by VPN or RADIUS

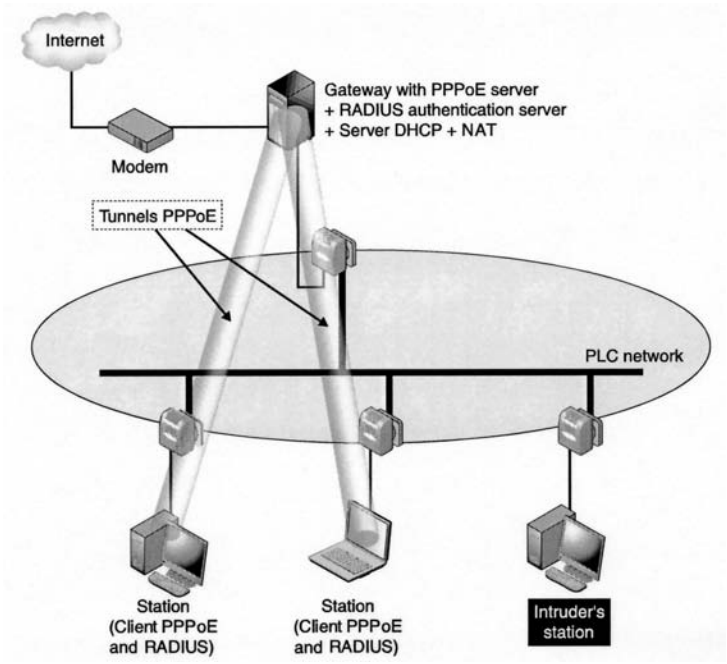

Figure 10.19 PLC network with gateway protected by PPPoE and RADIUS servers

This protection technique based on PPPoE tunnels is widely used by Internet access providers to ensure the separation between the various Internet access clients but it can be applied to a PLC home or professional network as well.

Configuring an Internet Gateway

In a PLC network, any Internet connection may be used: 56K modem, ISDN, cable, ADSL, ADSL2+, satellite, or FTTH (fiber to the home). Since the transmission speed of a PLC network is between 1 and 14 Mbit/s for HomePlug 1.0, 1 to 85 Mbit/s for HomePlug Turbo, and 1- to 200 Mbit/s for HomePlug AV, the throughputs of the Internet connections currently available are largely covered.

The HomePlug 1.0 performance can generate useful throughputs that are lower than those of the latest ADSL technologies such as ADSL2+ (20 Mbit/s); but as soon as you switch to HomePlug Turbo (25 Mbit/s), this is no longer a problem.

The Internet connection can occur in two different ways:

- By using a dedicated computer, or by connecting the PLC device directly to the modem for access to the Internet or InternetBox;
- By using a PLC modem-router directly.

In the first case, a computer shares its connection, as illustrated in Figure 10.20.

Figure 10.21 illustrates a PLC home network in which a multifunction device (xDSL/PLC modem/router) is connected to the Internet.

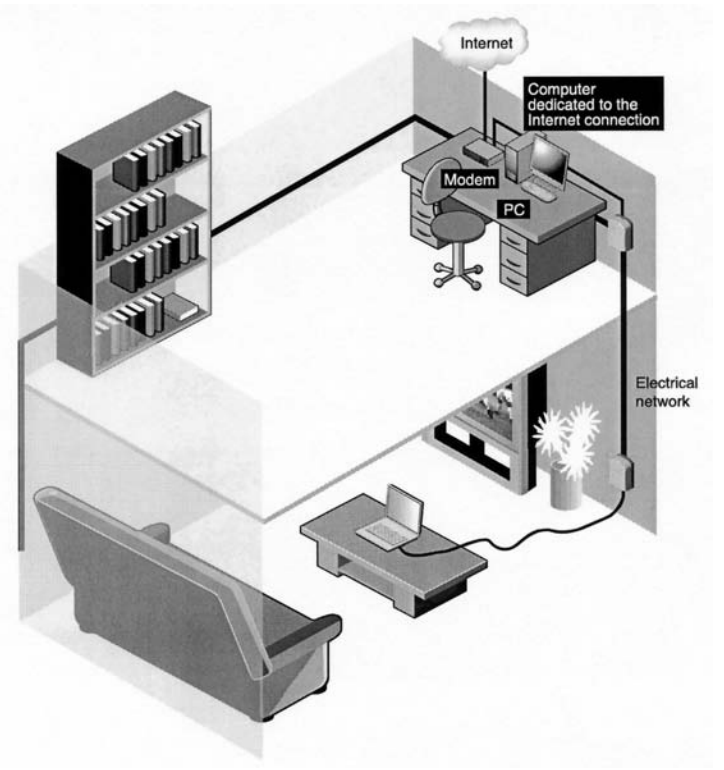

Figure 10.20 Internet connection via a dedicated computer

The disadvantage of this type of typology is that the PLC device only rarely has a firewall used for blocking various traffic types and avoiding attacks on the network or a VPN. In a topology where a dedicated computer is used for the Internet connection, any firewalling software or VPN server can be installed to protect the network.

Sharing the Internet Connection

For sharing an Internet connection, two protocols are used: the NAT (network address translation) and the DHCP (dynamic host configuration protocol):

- NAT enables the sharing of an Internet connection between several stations while using the IP address given by the Internet access provider (IAP). Another distinctive feature of the NAT is that this enables you to prevent certain attacks. Some Internet modems fitted with router functionalities incorporate the NAT, but it can be installed on a dedicated computer connected to the Internet.
- DHCP is a client-server protocol that enables you to dynamically allocate, for a given amount of time (lease time), the TCP/IP parameters that a station requires for its connection to the network. The parameters given by the DHCP server to the station are the computer IP address, the subnet mask, the address of the default gateway, and the addresses of the name servers (DNS). DHCP

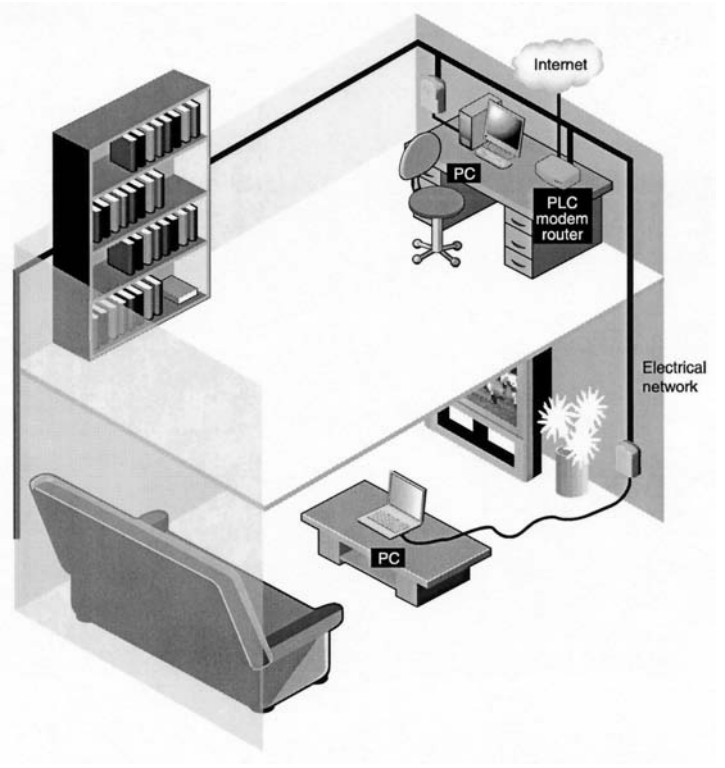

Figure 10.21 Internet connection via a PLC modem-router

offers a user-friendly station configuration mode, but this configuration can also be performed manually by modifying the board parameters directly.

DNS Addresses

The DNS addresses are given by the Internet access provider, except if there is a local DNS in the home network.

As far as IP addresses are concerned, all the network stations must have the same network address, e.g., 192.168.0.x or 10.0.x.x, with x between 1 and 254 in both cases, as illustrated by Figure 10.22.

Configuring NAT and DHCP

The ideal architecture of a PLC home network is the architecture in which the PLC router is used both as the NAT router and as the DHCP server, with the NAT enabling the sharing of the Internet connection with all the devices connected to the network and the DHCP giving all the parameters used by each device for its connection to the network. These functionalities are available with most PLC modems-routers intended for the domestic market.

This ideal architecture is illustrated in Figure 10.23.

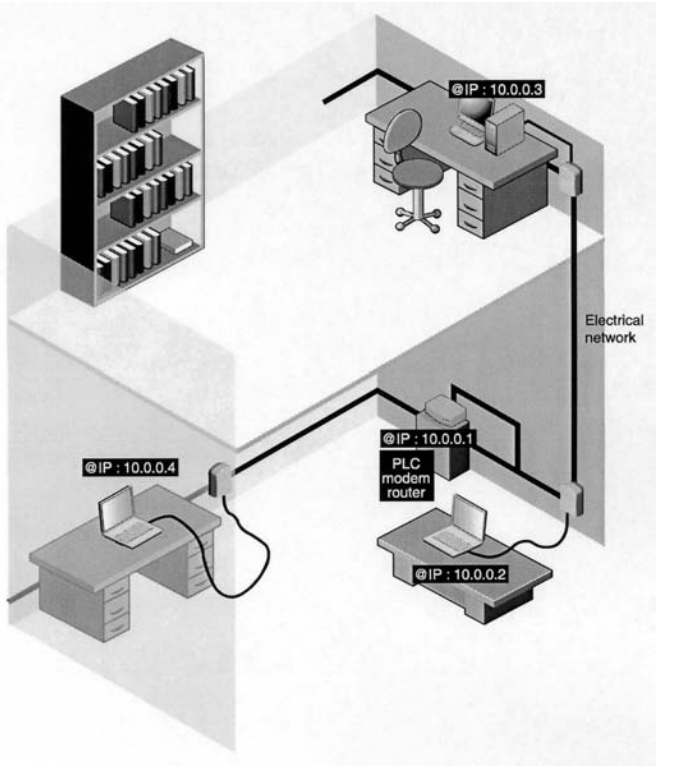

Figure 10.22 Configuring home network IP addresses

In the case where NAT and DHCP functionalities are not built into the Internet modem or the InternetBox used as an Internet access gateway, it is still possible to use them, but by configuring a dedicated computer acting as a gateway, as illustrated in Figure 10.24.

To configure such a dedicated computer, the best solution is to use Linux, the various distributions of which provide NAT and DHCP functionalities, whereas chargeable software must be used under Windows. The other advantage of Linux is that the system does not require tremendous resources.

To configure a computer using NAT and incorporating a DHCP server, a 486 generation processor and 32 Mb of memory are more than enough. Another advantage: this computer can remain switched on all the time without encountering any bugs.

DHCP (Dynamic Host Configuration Protocol)

The DHCP protocol is used for dynamically providing IP parameters to the stations connecting to the network. This protocol is used more and more since it makes network administration easier, in particular when a rather high number of computers are administered.

DHCP was originally designed to complete another protocol, BOOTP (Boot strap Protocol), used in the same spirit. The BOOTP messages are compatible with DHCP but not the reverse. The difference between DHCP and BOOTP is that

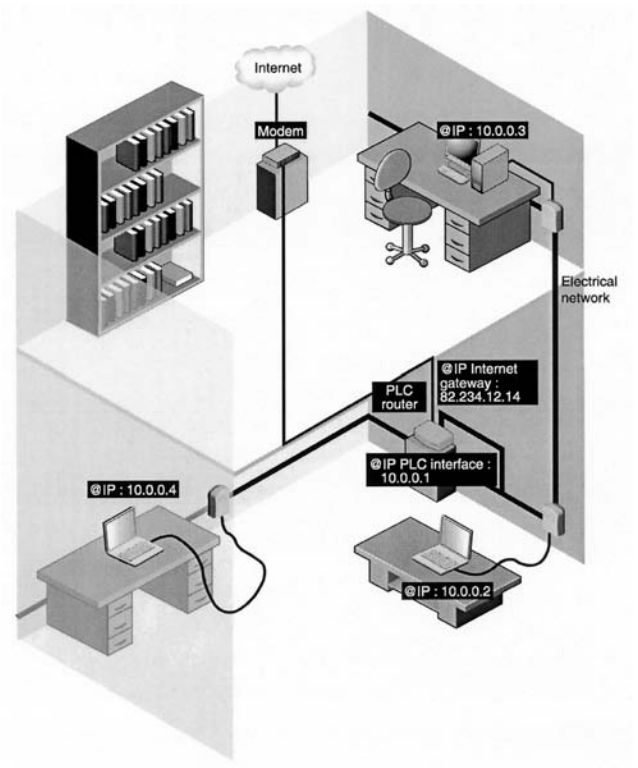

Figure 10.23 Ideal architecture of a PLC home network

DHCP can provide a station with a certain range of addresses and that each of these addresses is negotiated and is valid only for a given period of time.

DHCP Architecture

The DHCP is based on a client-server architecture. In the case of PLC networks, the DHCP client is the device connected to the PLC network and the DHCP server is the PLC modem-router.

In the example illustrated in Figure 10.25, there is only one DHCP server located at the InternetBox level for recent IAP offers or at the Internet modem level, but a network can be made up of several gateways for access to the Internet and therefore of several DHCP servers. Using several DHCP servers does not trigger any network constraints.

When a station initiates the DHCP protocol, this protocol provides it with the following parameters:

- IP address;
- Subnet mask;
- Default gateway;
- DNS address;
- Domain name.

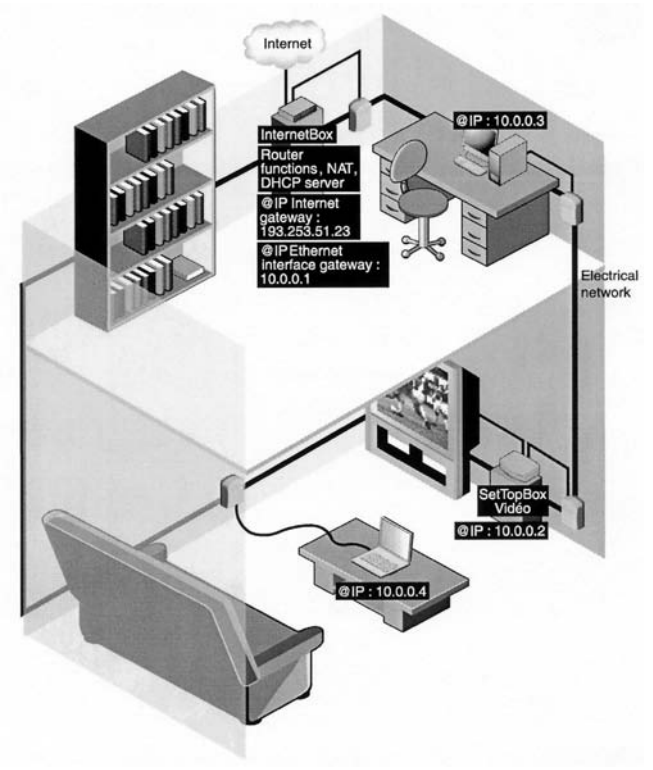

Figure 10.24 Architecture of a PLC home network with a dedicated gateway for accessing the Internet

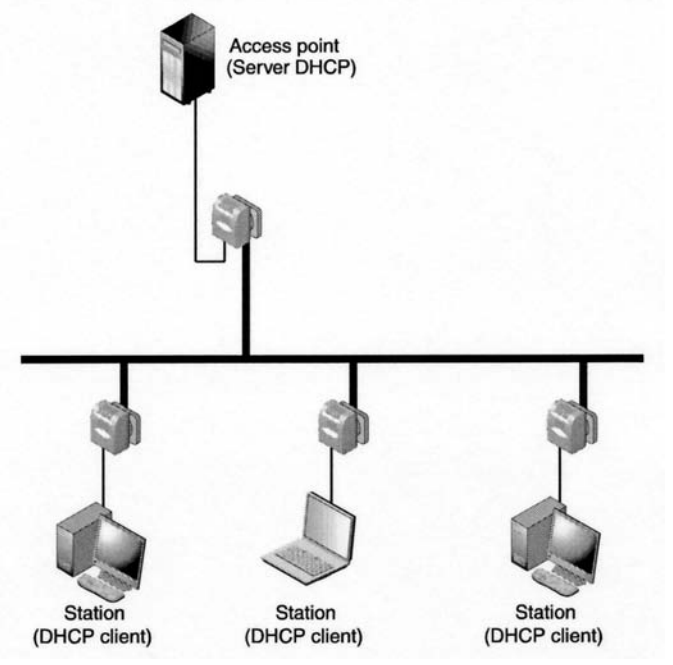

Figure 10.25 DHCP architecture

Once these parameters have been received, the computer can dialogue freely with other computers on the network or have access to the Internet if there is a connection sharing scheme. This is a user-transparent mechanism that does not take more than one second.

Another characteristic feature of DHCP is the lease. As we explained above, the parameters given to a network station are valid for a given period of time only. This lease is negotiated between the computer and the server when parameters are requested. When this lease expires, it can still be renegotiated by the computer.

Dynamic Configuration of a DHCP Client

The dynamic configuration of a computer that connects to a DHCP server takes place in four phases, as illustrated in Figure 10.26:

- When a DHCP client accesses a network, no address is allocated to him and his IP address is 0.0.0.0.
- In order to configurate himself, the client sends a DHCP DISCOVER request in broadcast mode – with IP address 255.255.255.255 – over the network in which he inserts his MAC address.

MAC Address

The MAC address is a fixed address assigned to each Ethernet board of the terminals connected to the PLC network.

- The DHCP server replies with a DHCP OFFER always sent in broadcast mode since the client does not have an IP address yet. The DHCP OFFER is made up of the client's MAC address, the lease time, and the server IP address.

It is possible to have several DHCP servers, but we only use one within the framework of this book.

- If the client accepts this offer, he sends a DHCP REQUEST in order to receive the parameters.
- The server sends a DHCP PACK confirming the client's acceptance.

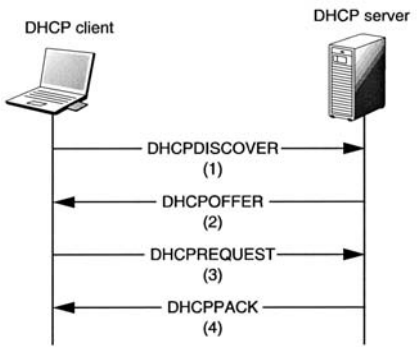

Figure 10.26 Dynamic configuration of a computer via the DHCP

Configuration Under Windows XP

Configuring a DHCP client under Windows XP is very simple:

- When inserting an Ethernet board under Windows, it is automatically configured as the DHCP client by default.
- If the board has already been configured before with a fixed IP address, open the Configuration panel and select "Network connection." The window illustrated in Figure 10.27 is displayed.
- Choose "Connection to the local area network" to display the dialogue box illustrated in Figure 10.28.
- Click on "Properties" to display the properties of the connection to the local area network, as illustrated in Figure 10.29.
- Tick the "Internet protocol (TCP/IP)" box. The "Properties of the Internet protocol (TCP/IP)" dialogue box is displayed, as illustrated in Figure 10.30.
- Tick the "Obtain an IP address automatically" box. The computer now has a DHCP configuration.

Under Windows 2000/XP, to check whether the board is configured properly, just make sure that it is supported in the "Status of the connection to the local area network" dialogue box, as illustrated in Figure 10.31 (see the first bullet above to access this dialogue box).

The "Details" button provides more information on the board's parameters (see Figure 10.32).

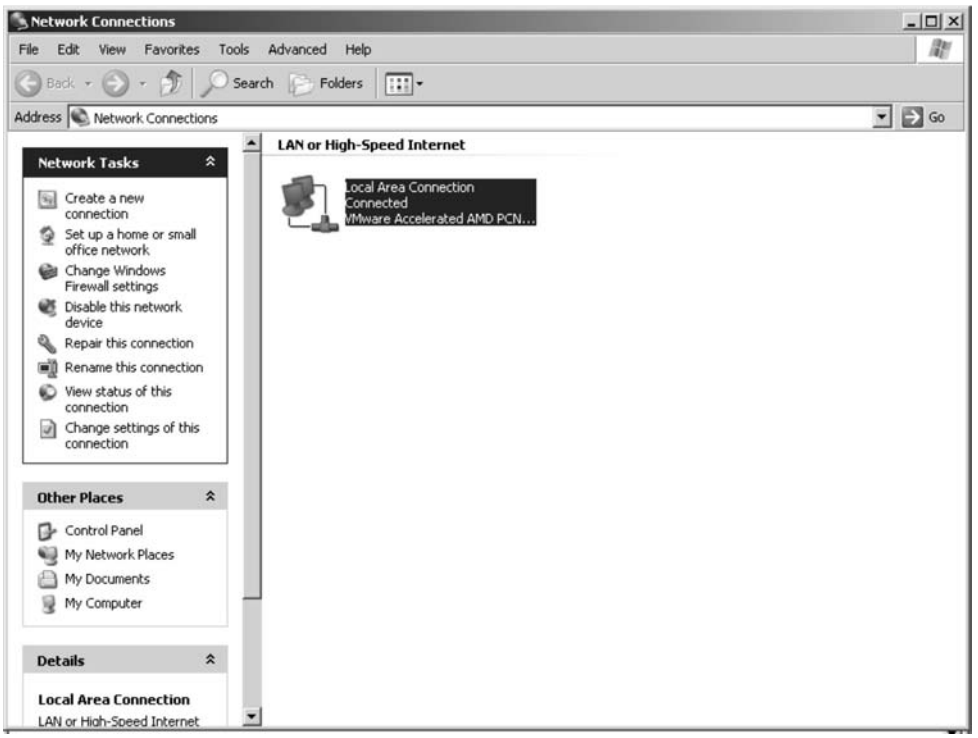

Figure 10.27 Network configuration (in this case, the PC also has a Wi-Fi connection)

Figure 10.28 Status of the connection to the local area network

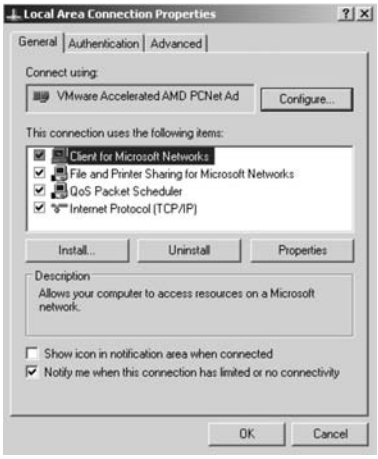

Figure 10.29 Properties of the connection to the local area network

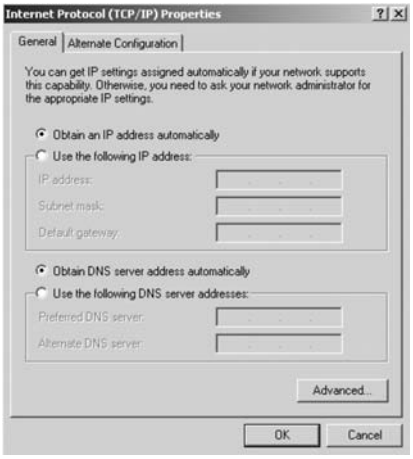
Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 10.30 Configuring the TCP/IP parameters of the local area network Ethernet board

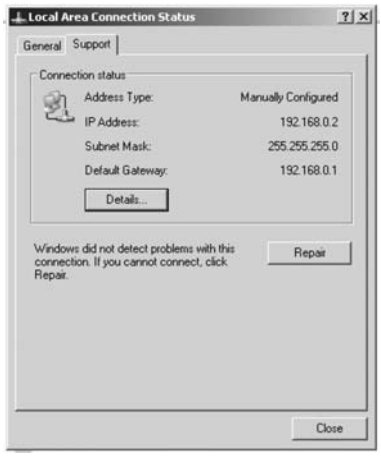

Figure 10.31 TCP/IP parameters of the local area network Ethernet board

The board configuration can be checked via the ipconfig command:

- In the Start menu, click on the "Execute" button, and enter cmd to open the MS-DOS command.
- When prompted to, enter ipconfig/all to display all the information concerning the network interface card and make sure that it has actually been configured. In Figure 10.33, we can see that the information is the same as that obtained previously.

The board may have not been configured by the DHCP server. If this is the case, Windows assigns a default IP address of the 169.254.x.x type to the board. To reinitialize a request to the DHCP server, just enter

```
ipconfig/release
```

then

```
ipconfig/renew.
```

Figure 10.32 Detailed TCP/IP parameters of the local area network Ethernet board

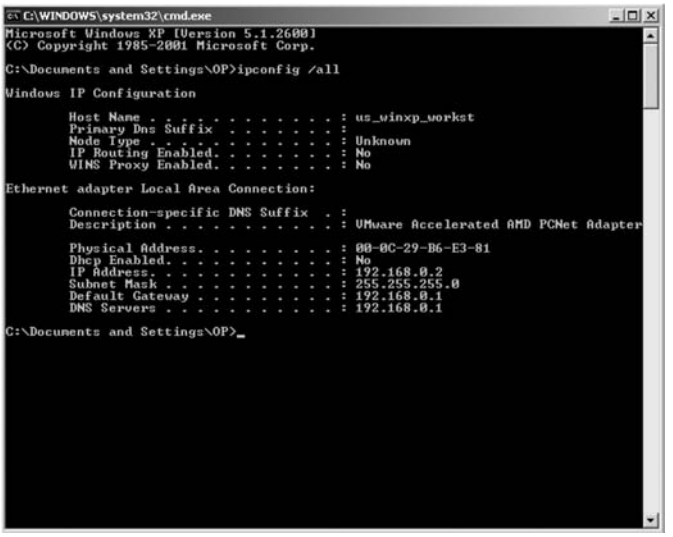
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\OP>ipconfig /all
Windows IP Configuration
Host Name . . . . . : us_winxp_workst
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . : 00-0C-29-B6-E3-81
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.0.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DNS Servers . . . . . : 192.168.0.1
C:\Documents and Settings\OP>

Figure 10.33 TCP/IP parameters of the board via ipconfig

CHAPTER 11

PLC for Businesses

The PLC networks increasingly invade the business world, and more generally the networks of professional and industrial buildings, where they complete or replace Wi-Fi or Ethernet networks.

The PLC networks can be considered as backbones not only for the premises of a SMB but also for professional (hotels, hospitals, concert halls, superstores, and so forth) and industrial (factories, warehouses, cranes, and so forth) buildings due to the performance and propagation distances of the electrical networks.

Therefore, the PLC networks can be considered as a technology used for replacing, completing, or serving other corporate network technologies, in particular the following ones:

- Backbone to replace the Ethernet network for cost reasons or for buildings in which works cannot be carried out (classified or protected buildings, hospitals, and so forth) or backbone of a Wi-Fi network to connect the various cells of the radio system;
- Supplement to the Ethernet network to satisfy the needs for the extension of an existing network (lower costs, easy deployment, and so forth) or if a company moves;
- Temporary network for event coverage (such as a concert, conference, and so forth);
- Creation of several distinct networks on the same electrical network (administration, public corporation, laboratory, and so forth).

The price of PLC devices is not very high, especially in the case of a company fully changing over to the PLC technology when reasoning in the long term and if the savings related to the wired equipment are considered (cables, outlets, switches, and so forth).

Within a company, the PLC network can be considered either as an operating network or as a "guest" network used, for example, by visitors for gaining access to the Internet. In the latter case, it is preferable to separate this network from the corporate network.

As in the previous chapter devoted to the installation of a PLC home network, this chapter describes the necessary steps for the installation and configuration of a PLC corporate network with special emphasis on access to the electrical network.

Network Architecture

In a company, there can be great differences in the architecture of a PLC network according to the network size, to the number of stations to be connected, and to the objectives assigned to the network.

The network architecture of a small company with a small number of PCs (less than ten stations) and an Internet connection via a cable modem or ADSL does not differ from the architecture of a home network.

The single possible options relate to the management of the functionalities of the DHCP server, NAT router, and Internet connection via a dedicated gateway. Then, it is still possible to add one or several PLC gateways by means of a switch in order to build various PLC networks on the same electrical network.

Figure 11.1 illustrates an architecture in which the server acts as the DHCP server and NAT router and where a switch is connected to it to make it possible to add new PLC gateways for access to the architecture.

Most often, the PLC network comes along on top of an Ethernet network existing in a company that already has some functionalities, such as DHCP, the Internet connection, and NAT.

Figure 11.2 illustrates a corporate network consisting of two subnets connected to each other via a WAN (wide-area network) by means of routers. The routers are themselves connected to the Ethernet network of each section of the corporate network. The PLC networks used for connecting the terminals of the various company rooms are connected to these Ethernet networks.

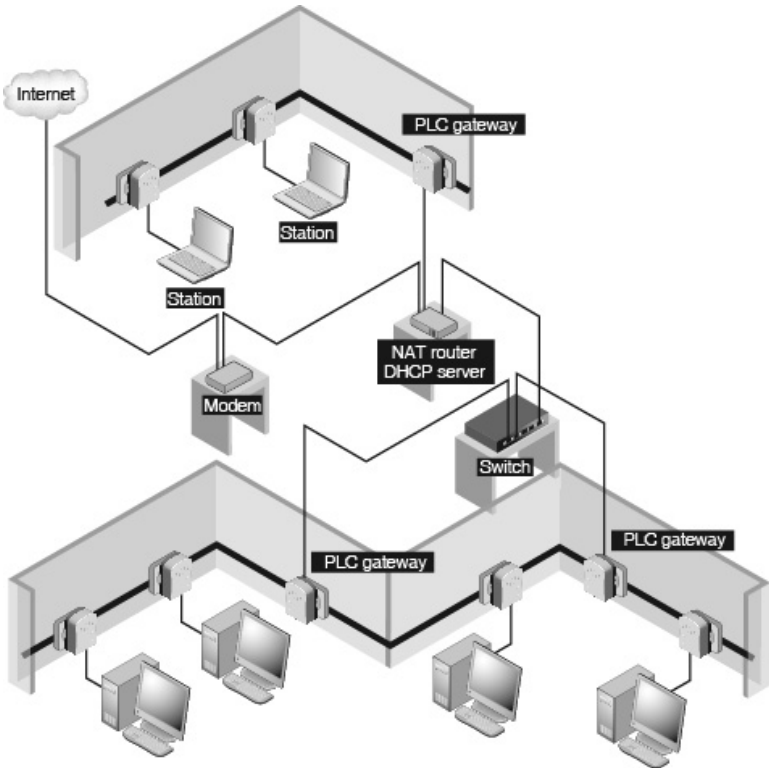

Figure 11.1 Architecture of a PLC network with several PLC gateways connected to a switch

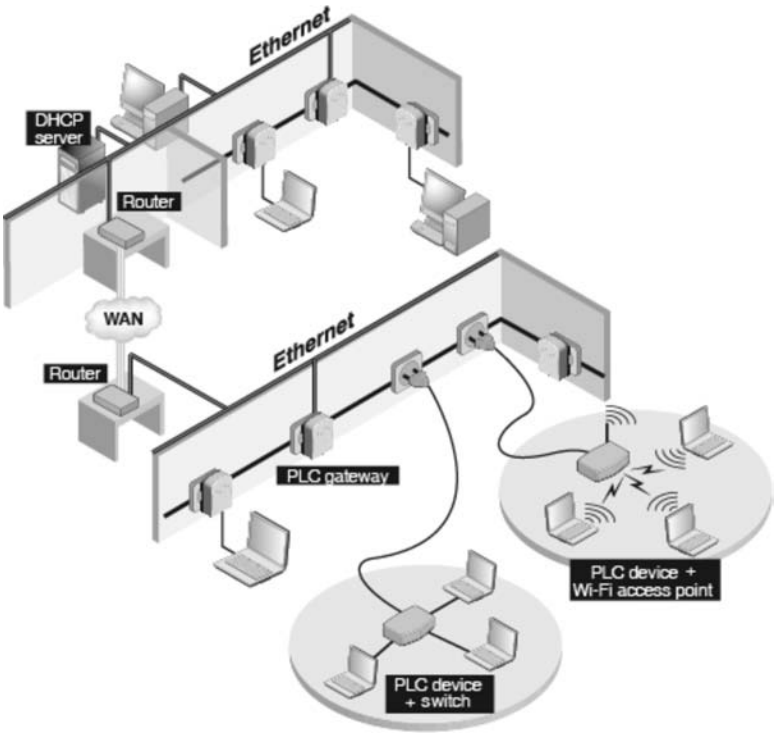

Figure 11.2 Corporate network architecture with routers incorporating PLC networks

The terminals can be connected to the network PLC devices in different ways as follows:

- Terminals directly connected to a PLC device connected to the electrical network;
- terminals connected to a switch PLC device that connects to the PLC network and distributes the connections in the room via its switch function;
- Terminals connected via their radio interface to a Wi-Fi access point fitted with a PLC functionality that it uses for its connection to the PLC network.

Supervising a PLC Network

The professional and industrial corporate networks require certain functionalities that are not demanded by home networks (supervision, in particular), in order to permanently ensure the good network operation and to retrieve alerts to the administrators should some devices fail.

Among the standardized protocols for supervision, the SNMP (simple network management protocol), versions v1, v2, and v3, has become prevalent in the network devices that are now largely fitted with a SNMP software element. This software element is used for interrogating a remote network device and for obtaining the value of a number of network and system parameters (lost packets, received packets, temperature of the boards, CPU polling, and so forth).

The PLC technologies operate at the data link layer level (MAC layer); they cannot be used for the direct remote SNMP interrogation. However, a number of hardware and software tools are used for supervising all the PLC networks.

Figure 11.3 illustrates the supervision of several PLC networks from various technologies. AsokaUSA, DS2, and Spidcom directly implement a HTTP interface and an SNMP stack (with the corresponding MIB) in their devices.

Since the HomePlug (1.0, Turbo, and AV) technologies do not propose an SNMP stack in their devices, it is necessary to use or to develop supervision tools at the MAC level and to use the PLC configuration tools that give the status of the PLC links at the PHY level.

Choosing a Standard

Unlike PLC networks for domestic use, for which the price of the devices is the main criterion, the professional and industrial corporate networks often require functionalities that imply the choice of a more professional technology while endeavoring to select a standard that is as open as possible to allow future evolutions.

Table 11.1 lists the criteria for the selection of a corporate PLC technology.

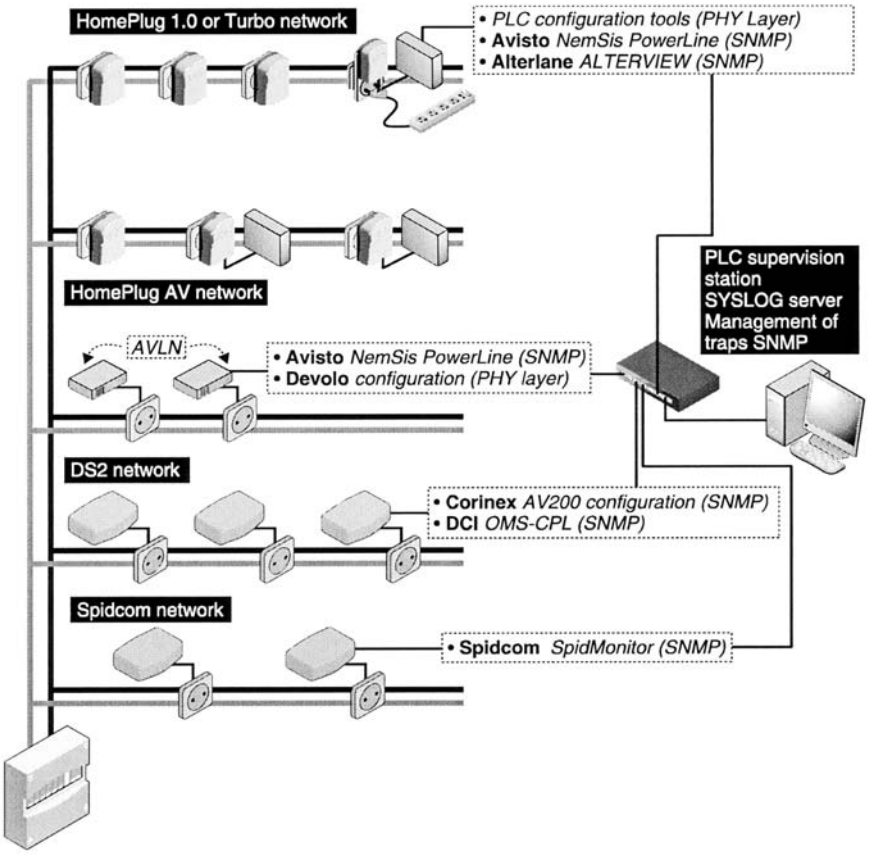

Figure 11.3 Supervision tools for the various PLC network technologies

Table 11.1 Criteria for the Choice of Corporate PLC Technologies

PLC TECHNOLOGY		*CHOICE CRITERION*
HomePlug	1.0, Turbo	Low cost, ideal for SMB, few advanced functionalities, DES 56-bit security, easy deployment, few administration possibilities
	AV	Leading-edge technology, high useful throughput, higher cost, advanced network management functionalities, guaranteed QoS
	AsokaUSA	HomePlug 1.0 and Turbo compatible, advanced functionalities (HTTP interface, SNMP administration with a single IP address, reinforced security, and so forth), professional electrical coupling systems, PLC repeaters
DS2 AV200		High and stable throughput, master-slave architecture, centralized administration, not HomePlug compatible, product integration into professional packages, advanced configuration functionalities (security, QoS, VLAN, and so forth)
Spidcom		High and stable throughput, highly advanced configuration (possible configuration of each of the frequency sub-bands used), centralized administration (SNMP, HTTP, and so forth), experience with innovative products in the PLC field

The AsokaUSA company develops products intended for professionals based on the HomePlug specification, which makes these products interoperable with the HomePlug 1.0, Turbo, and AV devices. This company also proposes products and accessories used for optimizing the PLC network (repeaters, filters, coupling systems).

The Devolo company develops HomePlug (1.0, Turbo, and AV) products intended for professionals by integrating them into metal packages fitted with attachment systems suited to the technical rooms close to the electrical devices of a company or industrial building.

Choosing Network and Electrical Equipment

Some criteria used for choosing PLC devices for home networks can be reused here, provided that a number of other criteria are added to them, in particular the following ones:

- Management of more than 15 devices (HomePlug 1.0 and Turbo standard limits for a simple PLC network);
- Network monitoring (typically SNMP);
- Centralized administration and configuration (HTTP, Telnet, SSH, and so forth);
- Isolated metal packages used for dissipating the heat of the PLC electronic components;
- PLC interface and separate 110 to 220V/50 to 60 Hz power supply;
- Possible repetition of the PLC signal;

- Integration of advanced network functions (NAT router, DHCP server, firewall, switch, Wi-Fi, and so forth).

As far as the PLC devices are concerned (filters, coupling systems, PLC signal injectors, and so forth), it is recommended to use professional products and to install them with the help of accredited electricians in order to ensure compliance with the security standards and to obtain a perennial installation.

Service Quality

The integration of the quality of service (QoS) into the various PLC technologies is required by the development of real-time applications, such as video on demand, broadcasting of HDTV video streams, IP telephony, computer-supported cooperative work, videoconferencing, and so forth.

The network constraints for such applications can be difficult to reconcile with the fact that the PLC technologies use as the communication medium the electrical network that is subjected to interference from the other devices connected to the network.

Table 11.2 summarizes the functionalities implemented in the various PLC technologies in order to satisfy these constraints.

Among these technologies, HomePlug 1.0 and Turbo are perhaps those offering the least QoS guarantees, whereas HomePlug AV offers optimal QoS guarantees, insofar as the PLC signal is based on the 110 to 220V/50 to 60 Hz signal conveyed over the electrical wirings to synchronize the various PLC network devices.

QoS in HomePlug AV

The HomePlug AV specification benefits from many developments and added functionalities in comparison with HomePlug 1.0 and Turbo. Among them, the QoS has been implemented by means of traffic classes with guaranteed performance. The AV name itself corresponds to audio and video, two application types in which the QoS constraints

Table 11.2 QoS Functionalities of the PLC Technologies

PLC TECHNOLOGY		*QoS FUNCTIONALITY*
HomePlug	1.0, Turbo	CA priorities (PRS intervals in the frames) corresponding to the VLAN labels of the IEEE 802.1Q standard
	AV	User priority classes (0 to 7) corresponding to the traffic classes of the IEEE 802.1D standard, Synchro AC, TDMA, QMP propagation, use of the VLAN labels of the IEEE 802.1Q standard
	AsokaUSA	PLC priorities (VLAN, fixed, fairness), priority levels (0 to 5), limitation by source (IP or MAC), by destination (IP or MAC) (uplink and downlink throughput)
DS2 AV200		Default priority, Criterion parameters, use of Offset, Pattern, Bitmask, use of the VLAN labels of the IEEE 802.1Q standard
Spidcom		Use of the IEEE 802.1Q (VLAN labels) and IEEE 802.1P standards for the QoS of time critical applications

(guaranteed high thrughput, propagation time, jitter) are crucial for the good transmission operation without data loss.

These constraints can be tolerated by implementing the following functionalities (see Chapter 3):

- PLC signal synchronization with 50/60 Hz in order to guarantee TDMA and CSMA/CA time spaces with CP (contention period) and CFP (contention-free period);
- QMP (QoS and MAC parameters) in the CM (connection manager), CCo (central coordinator) and STA (station) devices;
- Propagation of the QMP between the various network devices in order to keep the PLC network homogeneous in terms of QoS and performance.

Among the QMP parameters, Table 11.3 summarizes the most important ones for QoS management. As a reminder, the MSDU (MAC service data unit) is the data frame at the MAC level in the data link layer.

As we can see, the QoS management in HomePlug AV is particularly complicated and uses many parameters permanently exchanged between the network PLC devices.

This QoS management guarantees the network constraints that are required for the applications. HomePlug AV specifies eight application classes corresponding to various user priority levels, as indicated in Table 11.4.

Access to the Electrical Medium

As we have seen in Chapters 7 and 10, the two main methods for gaining access to the electrical medium are the following:

- Capacitive coupling, which consists of connecting the PLC device (gateway or network device) to an outlet like a home electrical device (see Figure 11.4).
- Inductive coupling, which is more efficient to broadcast the PLC signal over the cables and allows better performance. However, it requires access to the electrical wirings, which is only possible at the circuit breaker panel level by using couplers/injectors on each cable (on a single cable or several cables at the same time).

Figure 11.5 illustrates the principle of each type of PLC signal injection over the electrical wirings at the circuit breaker panel level. To place the PLC signal injection systems, it is preferable to remove the case of the circuit breaker panel in order to gain access to the various outgoing cables to the building outlets. To carry out this operation, it is necessary to be authorized to intervene on electrical networks or to call on an approved electrician.

Mutual induction phenomena between the electrical wirings of a network, in particular at the circuit breaker panel level, where the cables are close to each other, enable consideration of the system in different ways:

- A single cable (or a single phase or the neutral cable), with induction on the other cables.
- Several cables at the same time, with a single injector including all the cables and mutual induction to the neutral cable.

Table 11.3 Main HomePlug AV QoS QMP

QMP PARAMETER	*DESCRIPTION*
Delay bound	Maximum time measured in microseconds to convey an MSDU between the moment when it is delivered to the SAP (service access point) convergence sub-layer at the sending station data link layer level and the moment when it is received at the receiver station SAP layer level.
Jitter bound	Maximum shift measured in microseconds concerning the propagation delay of an MSDU between the SAP layer of the sender and the SAP layer of the receiver.
Nominal MSDU	Nominal value of the data part of the MSDU frame in bytes based on the IEEE 802.3 standard (between 46 bytes and 1,500 bytes).
Max MSDU	Maximum value of the data part of the MSDU frame.
Min MSDU	Minimum value of the data part of the MSDU frame.
Average data rate	Average transmission speed measured in 10-Kbit/s units specified at the SAP convergence sub-layer level to convey MSDU frames over a PLC link. This does not include MAC and PHY headers that are necessary to convey MSDU frames.
Max data rate	Maximum transmission speed specified at the SAP convergence sub-layer level to convey MSDU frames over a PLC link.
Min data rate	Minimum transmission speed specified at the SAP convergence sub-layer level to convey MSDU frames over a PLC link.
Max burst size	Maximum size, expressed in bytes, of an overrun during the continuous sending of MSDU frames generated by an application at the maximum transmission speed.
MSDU error rate	Error rate for an MSDU frame, expressed as $x \times 10^{-y}$, where x is specified in the 8 most significant bits in the unsigned integer format, and y in the 8 least significant bits in the same format.
Inactivity interval	Maximum time, measured in milliseconds, during which a connection may be maintained in the inactive status (no conveyance of useful data) before the CM (Connection Manager) device authorizes the transmission again.
CLST (convergence layer SAP type)	Compatibility of the SAP convergence sub-layer with other layers than that specified in the IEEE 802.3 standard.
CDESC (connection descriptor)	Optional fields from the upper application layers, or HLE (high layers entities), used, for example, for the QoS in the UPnP (universal plug-and-play) mode, or other upper application layers. These fields are the following: IP version (v4 or v6), source IP, destination IP, source port IP, destination port IP, IP protocol (UDP or TCP).
ATS tolerance	Tolerated variance, measured in microseconds, on the ATS (arrival time stamp) time stamping deviation between the PLC network synchronization clock or NTS (Network Time Base), and the marking of MSDU frames with the ATS time stamping.
Average number of PBs (PHY blocks) per TXOP (time allowed between two transmisson opportunities)	Average number of PHY data blocks (at the physical layer level) in 520-byte blocks per interval between two transmission opportunities to convey an MSDU frame over a PLC link.
Minimum number of PBs per TXOP	Minimum number of PHY data blocks (in 520-byte blocks) necessary to convey an MSDU frame over a PLC link.
Maximum number of PBs per TXOP	Maximum number of PHY data blocks (in 520-byte blocks) necessary to convey an MSDU frame over a PLC link.

- Each phase (each cable), with three different injectors connected to the cable TV PLC device via a "one-to-three" TV signal splitter. The induction takes place from the three phases to the neutral cable.

Table 11.4 Application Classes According to the User Priority Levels

USER PRIORITY LEVEL	*APPLICATION CLASS*
7	Network check (characterized by packets for which the reception is guaranteed in order to maintain the network infrastructure)
6	Voice (propagation delay of less than 10 ms and maximum known jitter–envisaged situation: campus LAN crossing)
5	Video and audio (propagation delay of less than 100 ms)
4	Checked network traffic (typically for professional applications with admission check and guaranteed bandwidth reservation during some transmission periods)
3	Platinium (typically for applications of the "best effort" type for some privileged users of the PLC network)
1, 2	Background traffic (typically for file transfers and other important traffic with no impact on the remainder of PLC network applications)
0	Best effort (typically the usual LAN traffic: electronic mail, Web navigation, FTP, IRC, and so forth)

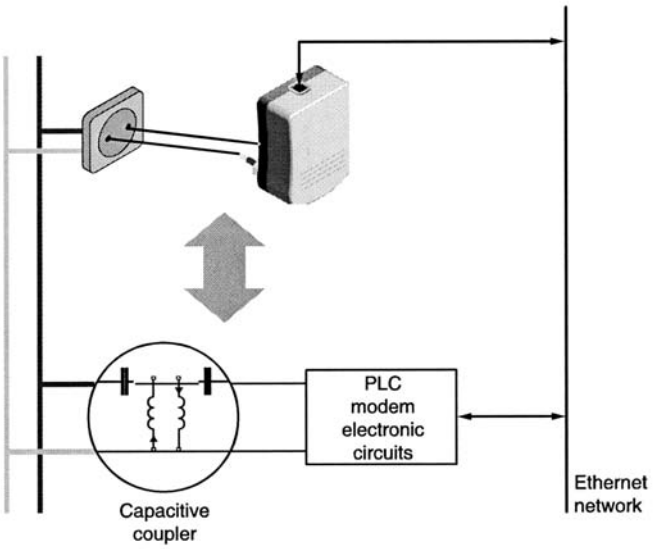

Figure 11.4 Capacitive coupling principle for a PLC device over the electrical network

Placing Equipment

The location of the PLC devices on the electrical network clearly influences the PLC signal propagation over the various electrical wirings running across a building. Therefore, it is important to choose a location that best promotes the propagation to the maximum network outlets, as illustrated in Figure 11.6.

The circuit breaker panel is a strategic place of the electrical network, since it can be viewed as the network "hub," where all the cables connect to recover the electricity from the meter. Therefore, this "electrical" hub is the ideal place for the placement of the PLC devices that will be used as the gateway, which will be connected both to the corporate Ethernet LAN and to the electrical network to broad-

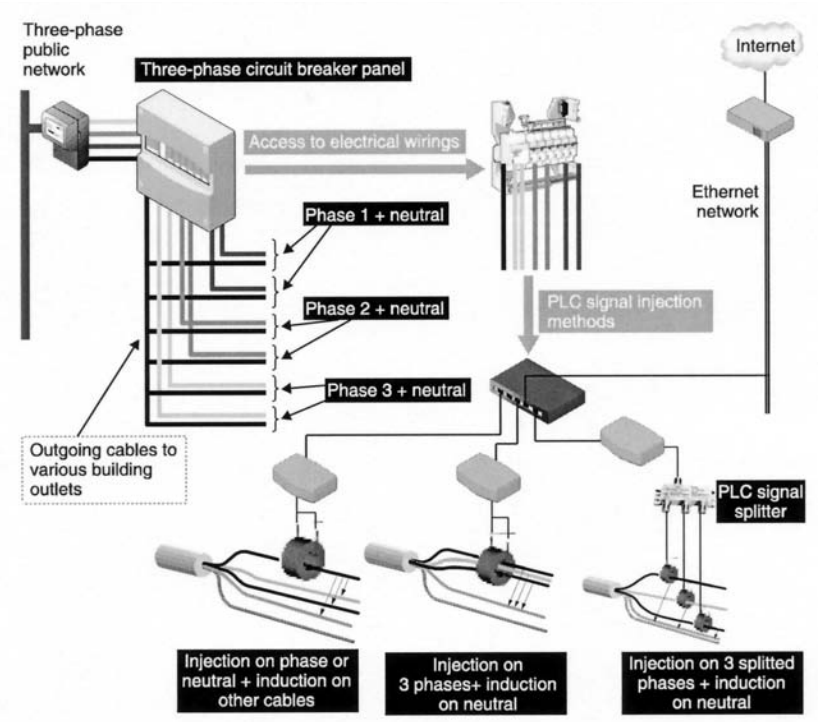
Three-phase public network
Three-phase circuit breaker panel
Internet
Access to electrical wirings
Ethernet network
Phase 1 + neutral
Phase 2 + neutral
PLC signal injection methods
Phase 3 + neutral
Outgoing cables to various building outlets
PLC signal splitter
Injection on phase or neutral + induction on other cables
Injection on 3 phases+ induction on neutral
Injection on 3 splitted phases + induction on neutral

Figure 11.5 Inductive coupling methods for PLC devices over electrical wirings

cast the Ethernet (Internet or LAN) frames to the various PLC devices connected to the outlets.

It is important to recover a wiring diagram of the building in order to know the topology of the electrical network and to see the various phase distributions (in the case of a three-phase topology).

Choosing the Network Architecture

As we could see in Chapters 3 and 10, there are several types of network architectures according to the PLC technologies used.

In the case of a peer-to-peer topology (HomePlug 1.0 or Turbo), one of the devices is used as the gateway between the Ethernet network and the electrical network, but has no specific place in the PLC network. This architecture type is relevant for LAN type networks connected between themselves by a wired Ethernet backbone.

Since each device has the same hierarchical level in the network, it is important not to space out the PLC devices too much on the electrical network (one device per adjacent room).

In the case of an architecture in the master-slave mode (DS2 or Spidcom), one of the devices (the master) benefits from a privileged place in the network and must be capable of displaying the various slave PLC devices. The circuit breaker panel is an ideal central location again to broadcast the PLC signal to the majority of the electri-

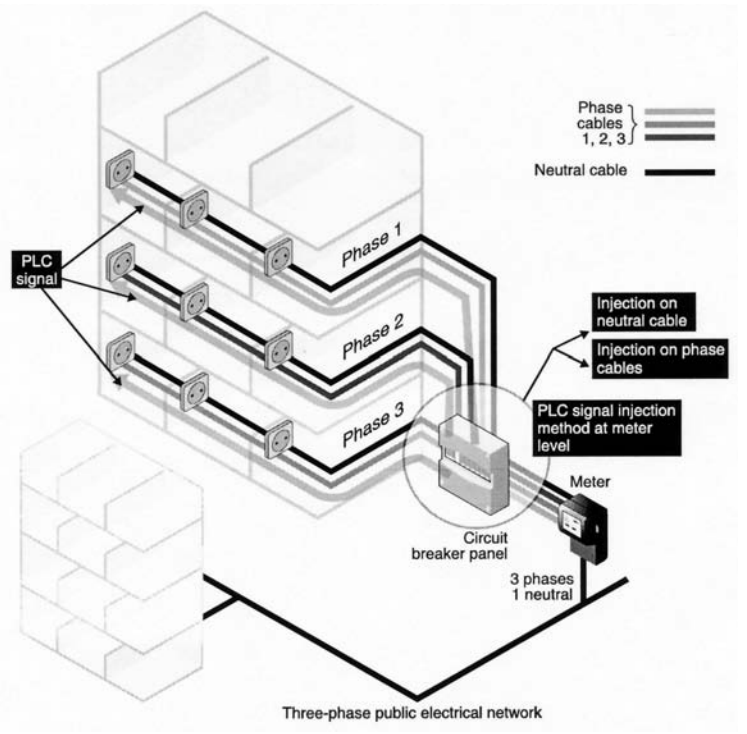

Figure 11.6 PLC signal injection at the circuit breaker panel of a building

cal network outlets. This central location can be in the technical room as close to the LAN Ethernet network devices as possible.

In the case of a centralized mode architecture (HomePlug AV), the architecture devices are the CCo (central coordinator) and the STA (stations). There is only one CCo per AVLN (AV logical network) to manage the PLC links between the network PLC devices. HomePlug AV specifies that the device best "placed" in the electrical network, i.e., the device that can view the other devices, is automatically configured as CCo because of its functionalities. Therefore, it is judicious to place this device at the most central point of the electrical network (circuit breaker panel) from which it can view all the STA devices of the HomePlug AV PLC network.

These various network architecture options are illustrated in the implementation example presented at the end of the chapter.

Security Parameters

As we have seen in the previous chapter dedicated to home networks, it is important to correctly configure the keys of the PLC networks so that no malevolent person can get into it and recover the frames circulating over the electrical network.

Let's specify that, unlike Wi-Fi technologies, which use the air and can therefore be potentially listened to, as the physical medium, the PLC technologies make it extremely difficult to connect to the electrical medium to try to recover these frames.

In the case of a company, it is however necessary to see to it that the firewalls for access to the Internet are correctly configured and that the various logical corporate networks are correctly separated in order to protect its data. The following sections introduce the main lines to be complied with for this purpose.

Security Topologies

There are radical methods to make a PLC corporate network secure, like the installation of the network fully outside of the corporate network or the access protection between the PLC part and the remainder of the network.

Figure 11.7 illustrates the first solution. It is generally expensive to install a PLC network outside of the corporate network in terms of time or equipment purchase. In addition, the company finds itself with two networks to manage and therefore two Internet connections, two DHCP servers, and so forth, the administration of which obviously requires more time.

In the second solution, illustrated in Figure 11.8, the connection between the PLC network and the corporate network is made secure in the same manner as an Internet connection by means of a firewall.

The AsokaUSA company proposes a PLC switch used for managing several HomePlug 1.0 and Turbo PLC networks. Since all the HomePlug 1.0 and Turbo devices support only one network key at a time, they cannot belong to several PLC networks at the same time.

Moreover, several HomePlug 1.0 and Turbo PLC devices cannot be separated in the same electrical network if they have the same network key. The only method to separate them is to enter a different network key on each of them and a PLC device

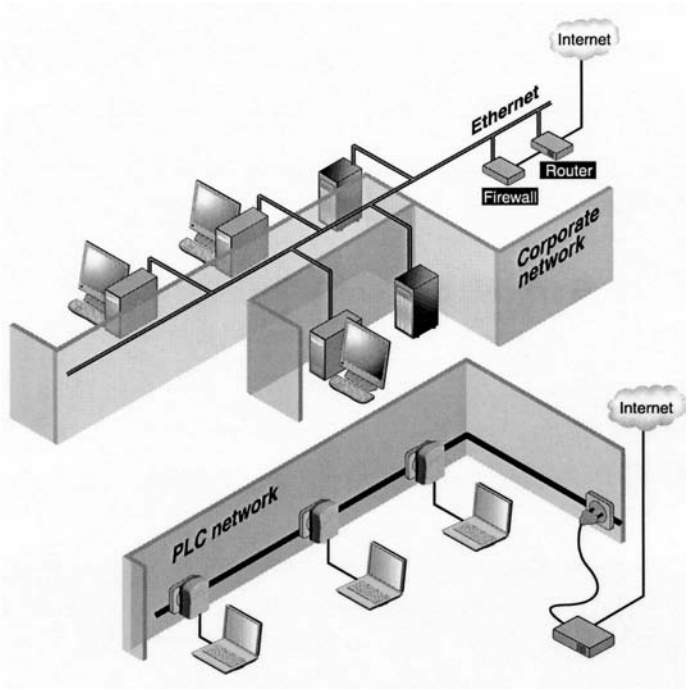

Figure 11.7 Architecture example for a PLC network not connected to the corporate network

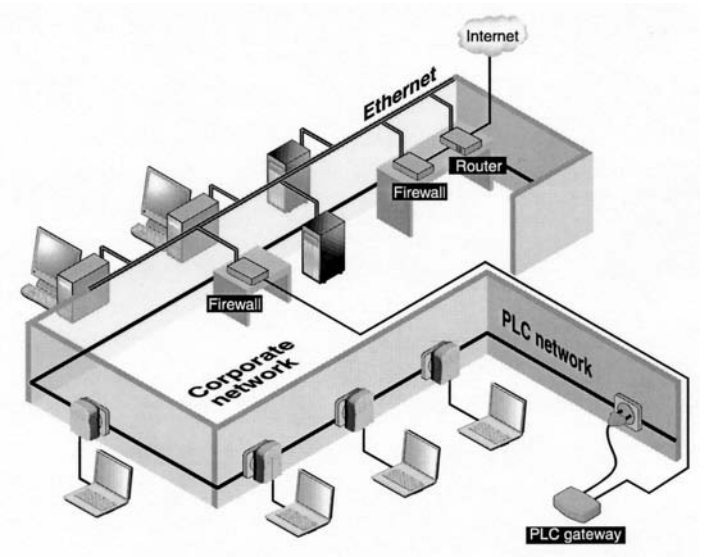

Figure 11.8 Architecture of a PLC network connected to the corporate network by means of a firewall

as a gateway capable of managing all these network keys. The 8950 switch from AsokaUSA does this by being capable of managing up to 253 PLC network keys and 1,024 users at the same time. Information on this product is available at the following address:

http://www.asokausa.com/products/commercial/pluglan_8950.php

Management of Several PLC Networks and Separation of PLC Clients in HomePlug AV

Among the functionalities provided by HomePlug AV that are not available in HomePlug 1.0 and Turbo, the management of several network keys in the same device enables a PLC network to configure the central CCo device with several network keys and each of the other network PLC devices with a single network key. This implies that the PLC devices do not see each other and only see the central device used as a level 2 gateway for the network PLC components. So, an architecture of the FAI type can be created, in which each component of the network only has access to the Internet and not to the other components of the electrical local area network. Because of its flexibility, this PLC network type can be modified to enable the network components to place on the same IP network while having access to the Internet.

Configuring PLC Security

The security of a corporate network is essentially based on the collection of information and the monitoring used for determining the origin of an attack.

The important point of the PLC network security resides in the configuration of a correct network key for the optimum encryption of the data exchanged over the electrical network (in the case of HomePlug products, the NEK must be long and combine uppercase and lowercase characters as well as 20-character numerals).

According to the manufacturers of PLC devices and to the PLC technologies, it is more or less possible to configure advanced security functionalities. Table 11.5 summarizes the main security functionalities of the various PLC technologies.

VLAN (Virtual LAN)

As its name indicates, a VLAN (virtual LAN) is used for defining virtual local area networks. This technology, which has appeared for several years in Ethernet networks under the IEEE 802.1Q standard, enables the coexistence of several virtual local area networks over the same Ethernet connection.

Most corporate switches propose this solution, which is to graft a PLC network onto an existing Ethernet network. By creating two virtual local area networks, one for the Ethernet network and the other specifically dedicated to PLC, this solution results in the topology illustrated in Figure 11.8, in which both networks are separated by a firewall.

The PLC VLAN is based on the use of multiple network keys (NEK in the case of HomePlug) or of networks from various technologies (a HomePlug network and a DS2 network, for example). HomePlug supports the propagation of VLAN labels that can be configured on the switches of the company Ethernet network.

Virtual Private Networks (VPN)

As we have seen for PLC home networks, the VPN (virtual private networks) represent the most reliable way to make a PLC corporate network secure. For this purpose, they are based on a client-server architecture in which the client is the station connected to the PLC device and the server a dedicated computer.

Since this solution is detailed in Chapter 10, we do not go back to it here. Although the project is now fixed, FreeSWAN is the reference VPN open source solution. It is available at the following address: http://www.freeswan.org.

Installing and Configuring a PLC Repeater (Bridge)

As indicated before, the PLC signal propagates over the electrical wirings and is subjected to a significant attenuation due to the cable resistance and to the electromagnetic disturbances caused by the electrical devices connected to the electrical

Table 11.5 Security Functionalities of PLC Technologies

PLC TECHNOLOGY		*SECURITY FUNCTIONALITY*
HomePlug	1.0, Turbo	NEK (DES 56 bits)
	AV	NEK, NMK, DAK (AES-128 bits + key rotation)
	AsokaUSA	NEK, filtering by MAC address and IP address of the devices connected to the PLC network, password on the HTTPS configuration interface
DS2		Exchange of master-slave keys, filtering of MAC and IP addresses, password on the HTTP configuration interface
Spidcom		Exchange of master-slave keys

network. To remedy this attenuation problem and obtain an optimum and complete PLC signal coverage for a building, it may be useful to install devices called "repeaters" in order to extend the PLC network to the areas of the electrical network where the PLC signal attenuation is too high.

This section gives a configuration example for a repeater device used for extending the installed PLC network. The concept of a repeater device is correlated with that of a PLC network segment.

The architecture illustrated in Figure 11.9 includes the following PLC devices:

- PLC1 and PLC2 are PLT300 Oxance products active in PLRP mode specific to Oxance, which can be administered by means of a Web interface on the Ethernet network interface.
- PLC3 is a PLT320 Oxance product active in PRLP mode used for repeating the PLC signal over the electrical network. For this purpose, it has two HomePlug PLC interfaces but no Ethernet interface and can be administered by means of the PLC1 or PLC2 Web interface.
- PLC4 and PLC5 are usual passive HomePlug PLC products that cannot be connected to PLC1 and PLC2 without a repetition system.

Figure 11.10 gives a logical representation of this network with the various network segments connected to each other in order to provide a continuous PLC network on the entire electrical network.

The PLT320 has an IP address of 192.168.1.251. Once the configuration PC is correctly adjusted to be on the same IP network (192.168.1.100, for example), the connection is possible using the network password (default value is 0 ex works).

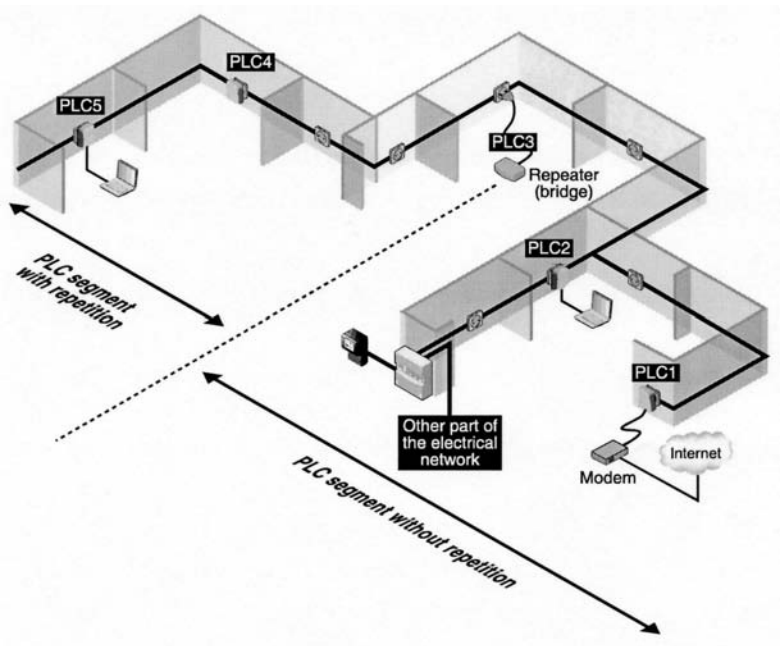

Figure 11.9 Example of network architecture requiring a repeated PLC signal

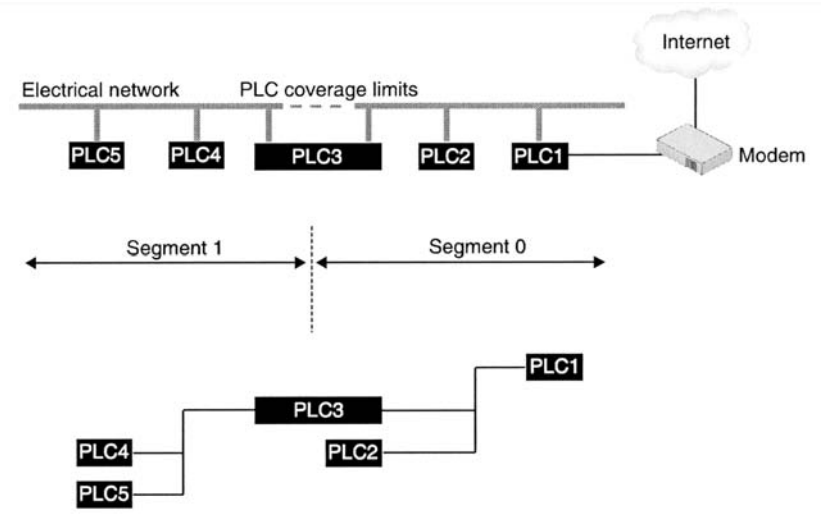

Figure 11.10 Logical representation of PLC repetition on two segments

To enable active PLC devices from Oxance to behave as a repeater (or bridge), an option must be activated by connecting to the PLT320 via the interface available on the PLT300 and by entering the MAC address of the PLT320 in the Source menu of the Oxance menu bar. A drop-down list displays the identified devices. These identifiers start with PLT and end with hexadecimal characters corresponding to the end of the MAC address (MAC address equal to 0c000b0507e8 for the device identified by PLT_0507e8).

Therefore, it is important to correctly read the MAC address on the case of the device to be configured and to spot it in the Source pull-down menu for connecting to it and modifying its configuration parameters. In this case, we spot the PLT320 device.

VoIP Under PLC

Since the PLC networks can be viewed as Ethernet networks in the electrical network, IP phones can be connected to it within the company. These phones are configured so that they can connect to a PABX (private automatic branch exchange) of the IP type. This PABX recovers the SIP (session initiation protocol) flows from the phones and is used as a gateway to the STN (i.e., the usual analog telephony network).

The royalty-free Asterisk tool developed by Michael Spencer, available at the following address: http://www.asterisk.org, can be installed on the corporate network in order to manage the IP phone fleet on PLC. The Digium company launched after the Asterisk project originated offers a range of services and products based on Asterisk implementations.

The advantage of this solution is that it makes it possible to move the IP phones on the entire electrical network. Figure 11.11 gives an architecture example.

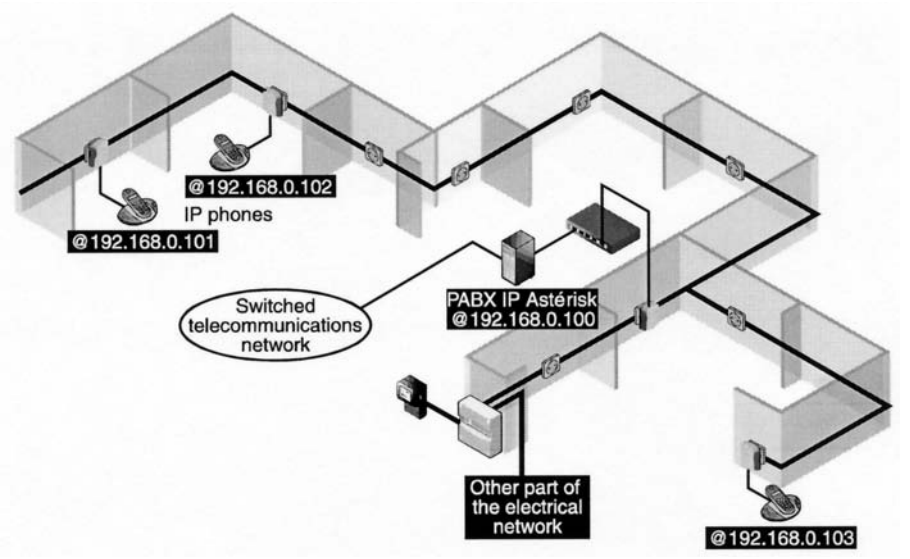

Figure 11.11 Infrastructure of IP telephony over PLC network

Sample Implementation of PLC in a Hotel

A hotel wants to be fitted with a multi-purpose computer network for the various services it proposes to its customers and decides to install a PLC network.

Figure 11.12 illustrates the hotel network architecture with two buildings supplied by a meter and two circuit breaker panels (one for each building).

Within these two buildings, the hotel manager wants the following services:

- Building A:
  - Internet access with data confidentiality in each bedroom.
  - Internet access and connection of the restaurant cash registers to the hotel information system.
- Building B:
  - Meeting room 1, which proposes an Ethernet local area network over PLC in order to allow exchanges between connected computers and a protected Internet access.
  - Meeting room 2, which proposes the same services as meeting room 1 but with compliance with the confidentiality of the data exchanged between the networks of both rooms.
  - Two rooms with public Internet access open to the hotel customers.
  - Conference room with IP videoconferencing solution via the PLC network.

Network Implementation

Implementing this network requires the correct display of all the logical networks connected to each other or not in the two buildings.

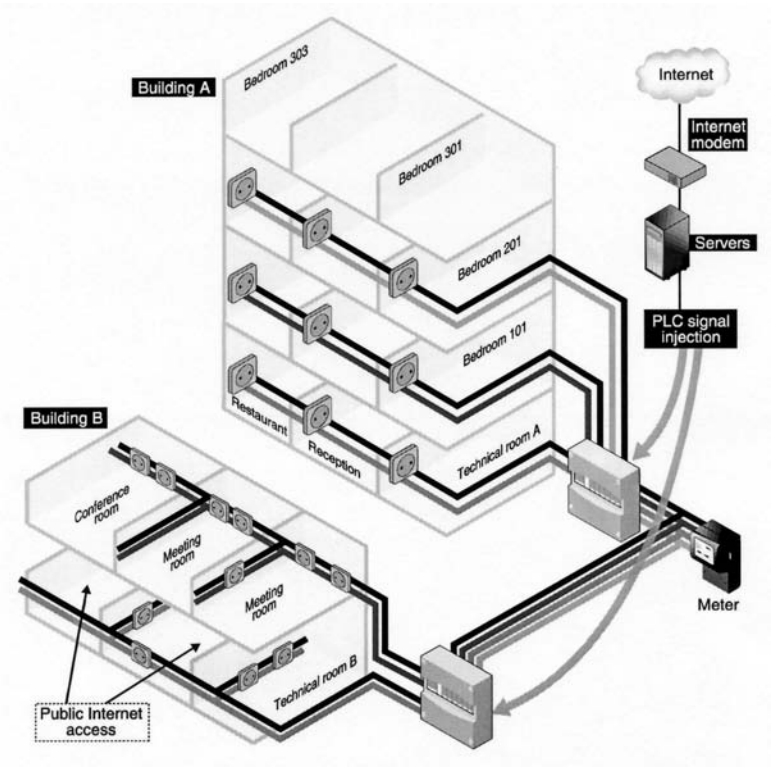

Figure 11.12 Hotel PLC network architecture

The following elements must be taken into account in the network architecture, as illustrated in Figure 11.13:

- Place and configuration of the various PLC gateways and PLC signal injection;
- Hotel Internet access;
- Network keys of the various PLC networks, whether separated or not;
- Network links between the buildings.

Figure 11.14 illustrates the overall logical architecture to be implemented. It includes wired Ethernet sections, like the link between the two buildings, since we want to maintain good performance in terms of throughput and a guaranteed service in order to avoid degrading the IP service in building B.

In order to separate the various PLC networks, it is important to place them on different phases if this is possible (three-phase cables and a neutral cable in the case of a three-phase installation) and especially to configure different network keys for each desired service. In terms of security, the installation of a RADIUS server can be envisaged in order to authenticate the PLC network clients.

This Figureure shows the connections of the PLC networks to the information system, especially the Internet accesses in the hotel bedrooms and the configurations with a NAT router for the meeting rooms used for protecting the customers' PCs and also the corporate network with respect to the administered PLC networks.

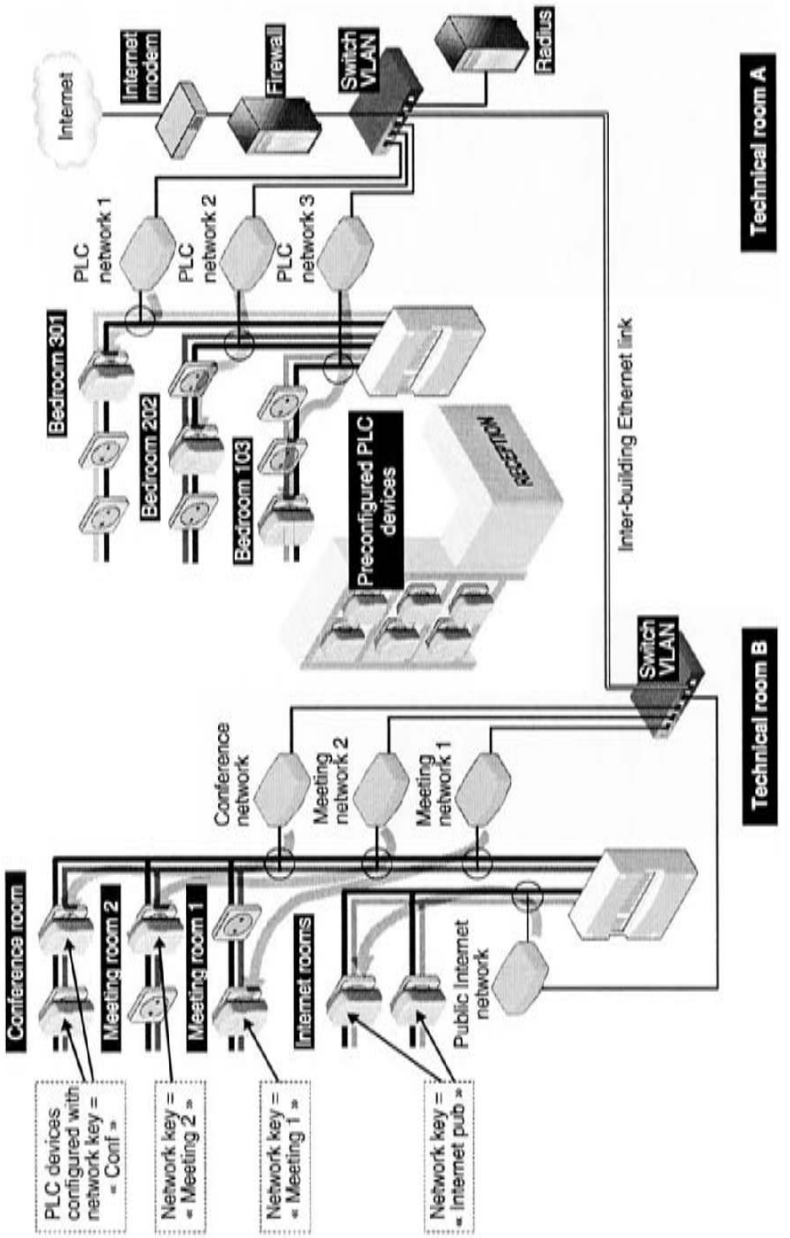

Figure 11.13 Complete architecture of the hotel PLC networks

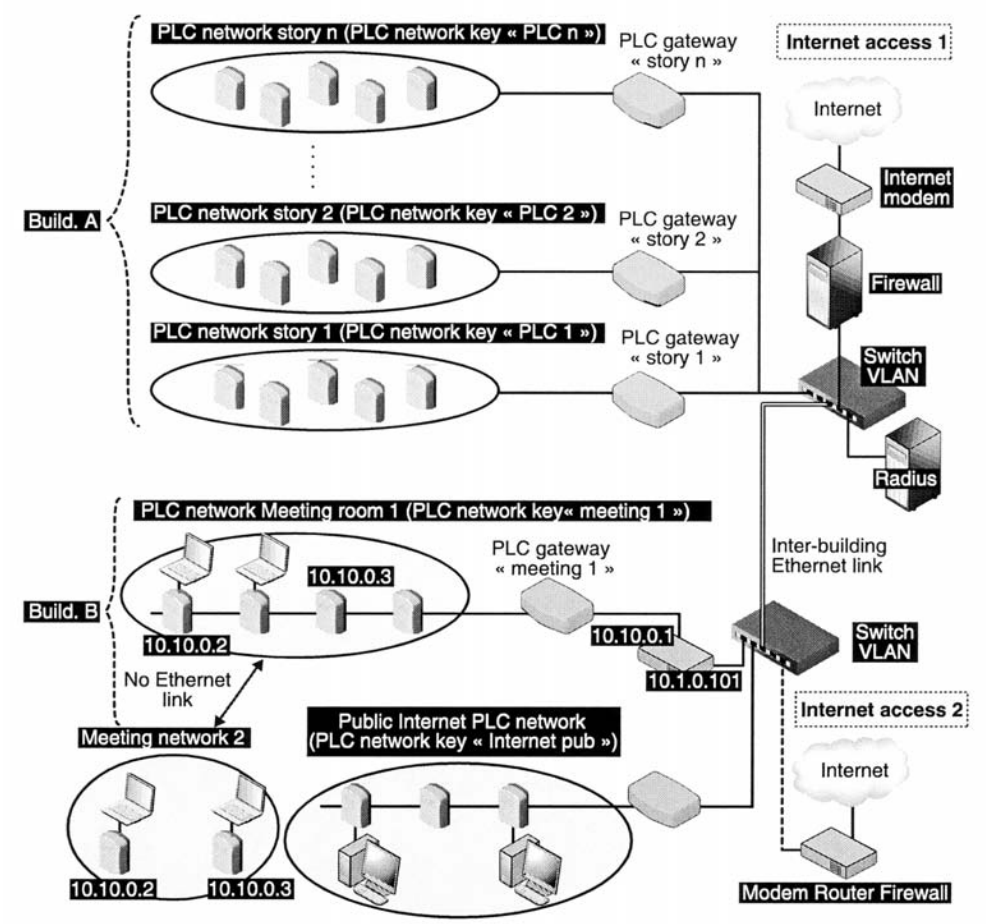

Figure 11.14 Overall logical architecture of the hotel PLC networks

Hotel Story PLC Networks

The hotel proposes to the customers to connect to the Internet in their bedrooms via a lent PLC device to be connected to the bedroom outlets. This connection to the Internet must take place in an authenticated, secured, and confidential manner. The PLC devices available at the hotel reception are, therefore, preconfigured so that they can connect to the PLC story network.

The technical problem raised is that HomePlug 1.0 and Turbo specify a limit of 15 devices for each PLC network behind a PLC gateway. Figure 11.15 illustrates the drawing of a story with more than 15 PLC devices that are potentially connectable to the hotel bedrooms corporate network with 22 bedrooms. The PLC signal is fed either by injection from the circuit breaker panel of the building or by pulling an Ethernet cable at each story and including a PLC gateway for each story if the distance is too high.

By using AsokaUSA 8950 products, PLC network extensions beyond the 15 device limit can be added with the creation of "segments," i.e., PLC areas with 15

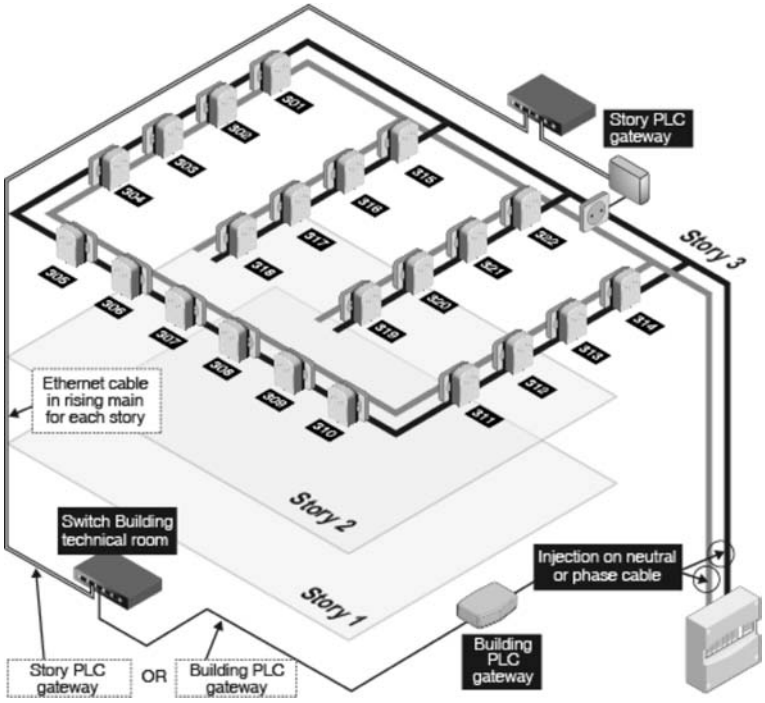

Figure 11.15 Managing the story PLC network with more than 15 devices

devices. For 22 bedrooms, it is just necessary to have two segments (one with 15 and one with 7) to cover the story requirements.

Figure 11.16 illustrates the PLC architecture to be configured for the AsokaUSA 8950 PLC device used for managing these 3 segments with 15 PLC devices.

Internet Access with Confidentiality Between Computers

One of the disadvantages of the PLC HomePlug 1.0 and Turbo networks comes from the fact that the medium is shared and that there may be network connections between network PLC devices, and therefore between bedrooms, as is shown by the case of the three bedrooms illustrated in Figure 11.17.

However, the data confidentiality can be ensured with the PlugLAN 8950 devices from AsokaUSA used for establishing blocking rules between the computers of the PLC network.

Let us suppose that the bedroom network is in 192.168.0.1/24. These rules are configured using the HTTP interface by means of the Security menu by selecting the Data filtering submenu and by ticking the Edit box. The new filtering rule must of course indicate the source and destination IP addresses of all the stations to be filtered.

The rule to be implemented must block the bidirectional IP traffic of any computer from network 192.168.1.0/24 to any other computer of the same network. An additional rule is necessary to authorize any bidirectional traffic to the outside networks.

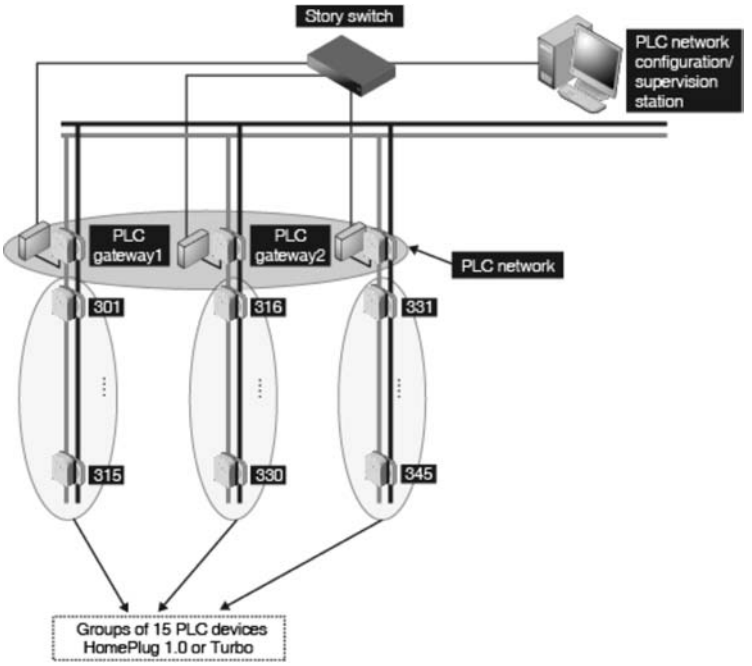

Figure 11.16 Story network architecture with several PLC segments

Configuring a DHCP Client Under Linux

Finding Linux systems in corporate networks, whether on servers or client stations, is more and more frequent. Therefore, it is important for the administrators of professional networks to know how to configure a DHCP client under Linux.

Before starting the configuration of the DHCP client, it should be ensured that the Ethernet board runs under Linux. If this is not the case, drivers must be installed for this board.

Under Linux, there are two widespread DHCP clients: dhclient and pump, which are available in all Linux distributions.

A DHCP client can be configured manually by entering dhclient eth0 or pump eth0, depending on the client concerned, with eth0 being the network interface, or automatically, by modifying the /etc/pcmcia/networks.opts file.

As in the case of Windows, just enter ifconfig eth0 to know the status of the board parameters and to know if this board is actually configured. If the board has not been configured by the DHCP server, no IP address appears:

```
# ifconfig eth0
eth0    Link encap:Ethernet  HWaddr 00:02:2D:4C:05:B8
        inet addr:10.0.0.2  Bcast:10.0.1.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        Interrupt:3 Base address:0x100
```

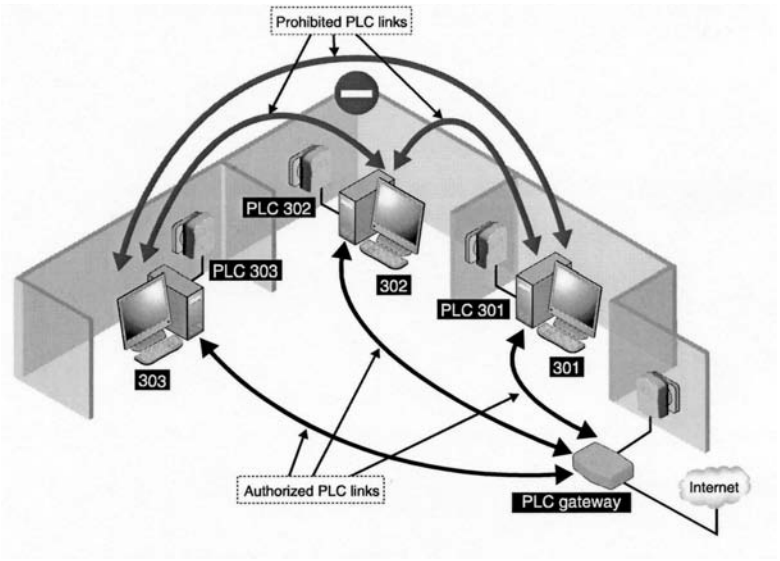

Figure 11.17 Internet access with confidentiality between computers

Configuring a DHCP/NAT Server

Most Linux distributions propose a DHCP server called dhcpd.

The configuration of the DHCP server just requires the creation of a dhcpd.conf configuration file which will be placed in the directory.

Here is an example of dhcpd.conf file:

```
subnet 10.0.0.0 netmask 255.255.255.0 {
range 10.0.0.2 10.0.0.50;
option routers 10.0.0.1;
option domain-name-servers 10.0.0.60;
default-lease-time 1000
max-lease-time 3600
}
```

- Subnet is used for defining the network address used by IP addresses.
- Netmask defines the subnet mask.
- Range defines the address range given by the dhcpd server.
- Option routers defines the IP address of the default gateway.
- Option domain-name-servers defines the DNS address.
- Default-lease-time defines the default lease time, in this case 1,000 seconds.
- Max-lease-time defines the maximum lease time.

The dhcpd server can be started whenever the Internet gateway is switched on by entering the following line:

```
# dhcpd eth0
```

where eth0 is the Ethernet interface connected to the gateway.

It can also be started automatically by creating a script in the /etc/rc directory and by incorporating the following command:

```
/usr/sbin/dhcpd eth0
```

NAT (Network Address Translation)

NAT is a technique used for connecting several computers to the Internet on the same IP address. NAT has been and still is widely used for compensating for the small number of available IP addresses.

Let us suppose a PLC network in which a PLC modem-router is connected to the Internet, as illustrated in Figure 11.18.

The network computers can only gain access to the Internet if the Internet modem or another entity in the network incorporates NAT routing functions and is connected to the Internet. Most of them incorporate the NAT.

The NAT routing makes it possible to use only one routable address over the Internet for a group of computers having non-routable, fixed private addresses.

When a computer sends data not intended for the local area network, the NAT router—the Internet modem in this case—replaces the IP address of the sender by the connection IP address given by the Internet access provider (@net on the figure). At the same time, the Internet modem writes the connection information (IP address of the sender, protocol used) to a translation table.

When the Internet modem receives data from the Internet, it checks the data receiver in its translation table by comparing the type of received data with the information contained in the table. Once the receiver is found, the IP @net address is replaced by that of the receiver. In this way, all the network computers use the same IP address for gaining access to the Internet.

The NAT can filter the incoming packets and avoid external attacks with this addressing scheme. If the connection is not initiated by the computers, the external packets cannot be processed by the NAT router.

NAT Configuration

Unlike the DHCP server, the NAT depends on the kernel used, 2.2 or 2.4/2.6. In both cases, and as for the DHCP server, it is possible either to start the NAT manu-

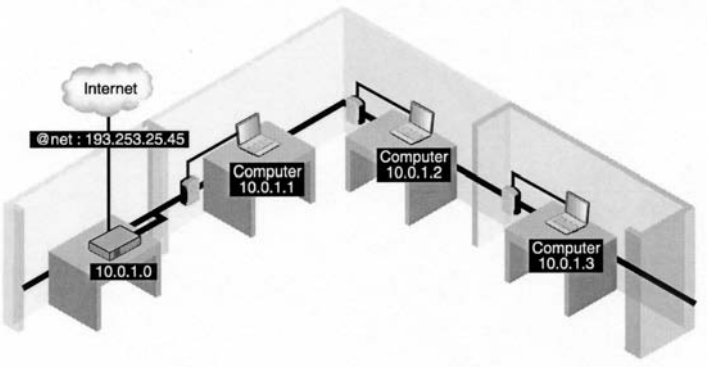

Figure 11.18 PLC network connected to the Internet

ally after having switched on the gateway, or to write a script in the /etc/rc directory in order to automatize the NAT execution when starting the gateway.

Irrespective of the kernel used, the /etc/network/options file must first be modified using the vi command, for example, and modifying the ip_forward=no line to ip_forward=yes.

For the 2.2 kernels, the ipchains command is used for managing the NAT:

```
/sbin/ipchains –A forward –i ppp0 –s 10.0.0.0/24 –j MASQ
```

ppp0 is the interface connected to the Internet.

For the 2.4 and 2.6 kernels, the iptables command must be used:

```
/sbin/iptables –t nat –A POSTROUTING –o ppp0 –s 10.0.0.0/24 –j
MASQUERADE
```

ppp0 is the interface connected to the Internet.

As indicated before, the PLC network can be viewed as a level 2 infrastructure (Ethernet) used for connecting the various IP terminals between themselves. The IP configuration of the devices connected to this network is therefore that usually found in all the IP networks (IP addressing, DHCP, and NAT functionalities, and so forth).

CHAPTER 12

PLC for Communities

During the last years, high throughput Internet accesses proposed by Internet access providers have spectacularly developed, providing both higher throughputs and new media to reach an increasing number of customers (telephone cable, TV cable, radio, and so forth).

Within this framework, and more especially in some countries throughout the world, the electrical network seems to be promising to convey the Internet signal as close as possible to the terminals wanting to connect by means of all the outlets of a building or apartment.

Using the public electrical network as the communication medium, and especially as the medium for the broadcasting of the Internet signal to the final customers has the obvious advantage that the electrical network is present everywhere. However, using this medium first of all designed for conveying and distributing the electrical signal as the telecommunications medium requires some precautions.

This chapter details the constraints and the chosen devices used for implementing a PLC network up to each user of the electrical network of a community. The installation of this type of infrastructure has already been implemented by some telecommunications operators.

Electrical Networks for Communities

As we have seen in the preceding chapters, the electrical networks in the broad sense can be considered as several subnets connected to each other with various voltage levels, various responsibilities, various managers, and various security levels.

As a first example, these subnets are regulated in the USA by the FERC and in France by the CRE (Commission de régulation de l'électricité) from the EHV (extra-high voltage) lines running across the country to connect the major electricity production sites to the various communities to the outlets in the buildings (houses, companies, and so forth) in order to supply the electrical devices that we use every day.

Figure 12.1 diagrammatically represents these various subnets, with their respective voltage levels and the associated line types, as well as their connection to the private electrical network downstream of the meter used for electrically connecting a building to the public network. The network of a community extends from the HV/MV transformer to the meters of the community buildings.

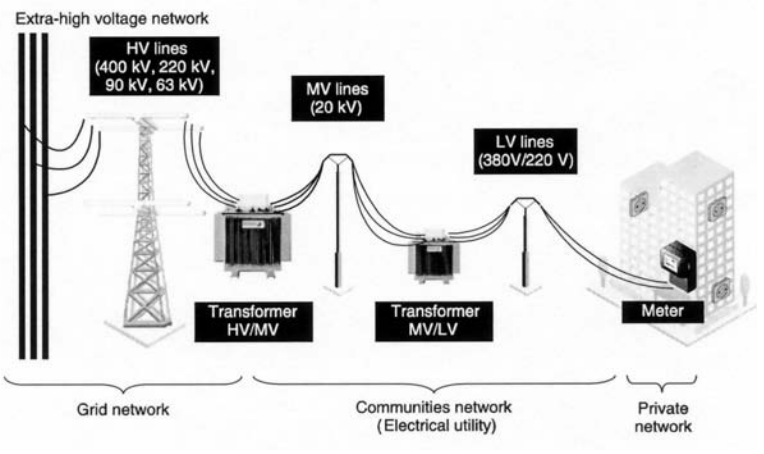

Figure 12.1 Architecture of electrical subnets

The various subnets of the electrical network partly differ by the network owner, on the one hand (cables, pylons, infrastructure devices, and so forth), which is in general the community for HTA electrical networks, and by the network operator, on the other hand, i.e. the one that uses, supplies, services, and maintains the network and the infrastructure devices forming it, generally an electrical utility for LV electrical networks.

Figure 12.2 illustrates this sharing of responsibilities for an LV network for the connection of the private electrical network to the public electrical network represented by the meter.

It is important to know this sharing of responsibilities should a PLC network be deployed, since the PLC devices must be installed on the various parts of the electrical network to allow PLC signal propagation from the IP network connection point to the outlets of the public electricity network users.

Electrical Network Operators

For an electrical network operator, whether local or national, or even international, which has electrical networks in some geographical locations only or distributed all over the country, the installation of a PLC network makes it a telecommunications operator like an Internet access provider for Internet accesses. This implies that it takes on the duties of a telecommunications network installer and manager within

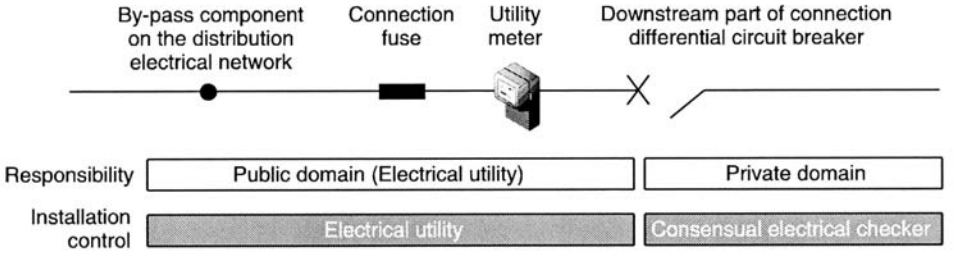

Figure 12.2 Sharing of responsibilities for an electrical distribution network

the framework of an electrical network that has safety rules different from those of twisted pair, cable TV, or optical fiber networks.

For electrical utilities managing the local electrical networks (village communities, small towns, built-up areas, commune syndicates, and so forth), the PLC can represent the best technology to connect the local authorities located in white areas to the Internet.

The latest deployments of PLC networks, whether experimental or operational, have demonstrated that this technology could efficiently help the communities to provide Internet access to homes that could benefit from Internet access. These deployments are often based on local telecommunications operators by means of network architectures using the best of each currently available technology (BLR, Wi-Fi, PLC, mesh network, and so forth).

Sometimes, the electrical utility prefer to confine itself to the electrical power production, transport, and distribution businesses with which it is familiar, and not to place itself as a potential telecommunications operator for the thirty million or so meters connected to its network. Moreover, this decision could be based on the local political directives concerning the specialization principle of each of the electrical utilities and electrical grid systems.

Topology of Electrical Networks

Several construction rules govern the implementation of a "distribution" electrical network, i.e., connected to the major high voltage networks, or HV, supplying the buildings of a community by providing electricity to the subscribers' meters.

First, a distinction can be made between three types of MV and LV electrical networks according to the building density and the geographical area under consideration (see Figure 12.3): rural, semiurban, and urban.

The specificities of these electrical networks relate to the following elements:

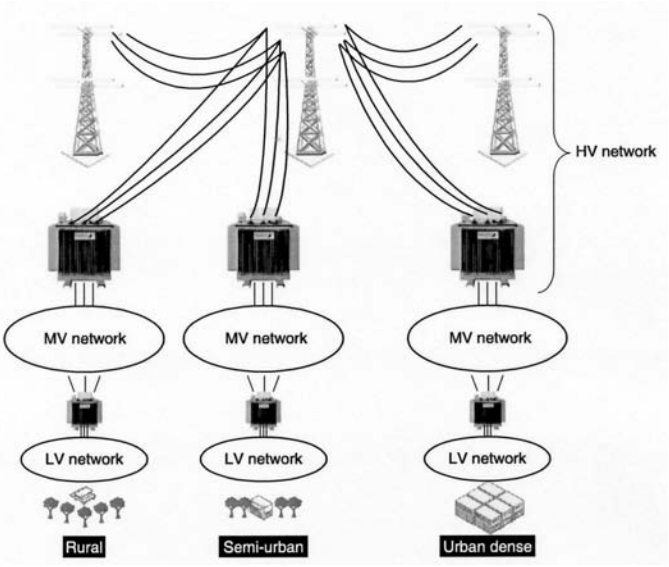

Figure 12.3 MV and LV electrical networks

- Network topology;
- Distance between pylons;
- Distance between the transformer and the various meters that it supplies;
- Number of meters behind a MV/LV distribution transformer.

For each of these networks, three MV electrical network topologies are possible: star, ring, or mesh topologies. The most widespread topology is the mesh topology, which has the advantage of protecting the entire electrical network against possible electrical defects at some points of the network. If a defect, like a short circuit, weakens the network at a point, other electrical lines take over since the topology provides backup links due to meshing. No point of the electrical network is supplied by a single electrical line.

Topology of MV Networks

In rural areas, the star topology of the "tree" type is widespread. In semiurban areas, star topologies of the "tree" type and ring topologies are found with several high voltage network connection points.

In dense urban areas, the widespread topology is the mesh topology, but it operates as an energized star configuration. The mesh links are backup links should one of the main links be cut.

Figures 12.4 to 12.6 illustrate these various MV network topologies.

Topology of LV Networks

In most countries, the topology of LV electrical networks is a star topology of the tree type allowing links in this way by meshing between certain branches of the electrical network. However, these mesh links are still too rare to define the network topology as an actual mesh.

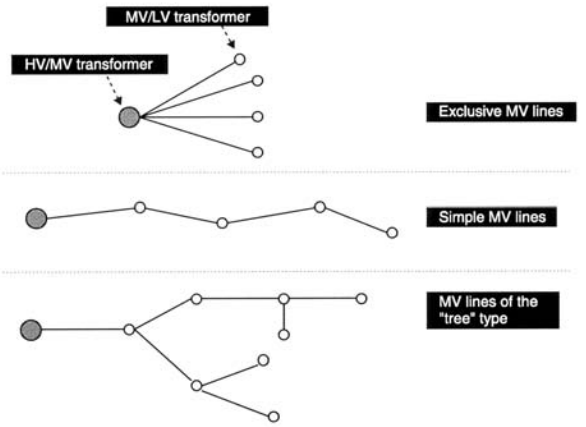

Figure 12.4 Star topology

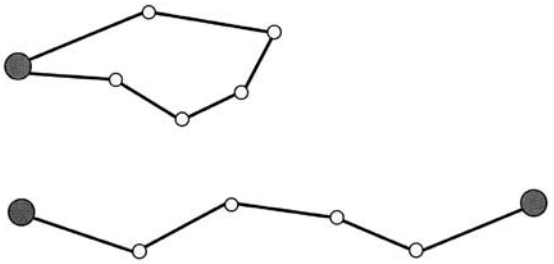

Figure 12.5 Ring topology

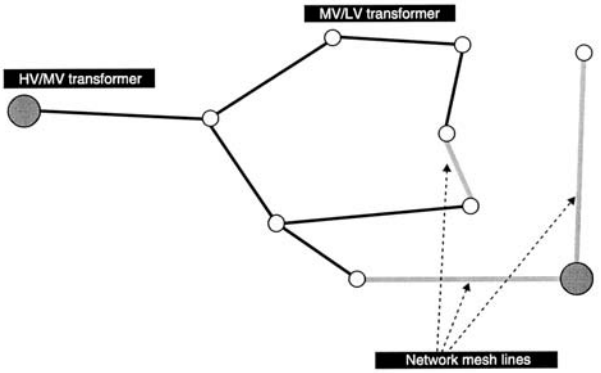

Figure 12.6 Mesh topology

The electrical network construction rules determine the PLC engineering to be implemented to obtain the best coverage and the best performance of the IP network to the subscribers and the outlets of the community buildings.

Figure 12.7 illustrates an electrical network representative of a community from the MV/LV transformer to the various branches of the LV (low voltage) network supplying the subscribers' meters.

If we take a closer look at the topology and the electrical devices of a power line distribution system in a dense urban environment (dwelling meters supply, for example), we find again the situation illustrated in Figure 12.8. This very complete Figureure shows the various components of the electrical network from the local electrical substation to the meter in an apartment. The PLC devices used for broadcasting the data signal from the electrical substation to the slave PLC device in the apartment are superimposed on this electrical installation.

Implementation of a Communitywide PLC Network

Various issues must be considered when installing a PLC network for a community. To begin with, a project team is set up, with a contracting authority (in this case, the community defining the requirements in terms of Internet access and IP network in order to prepare the specifications) and a prime contractor defining the engineering

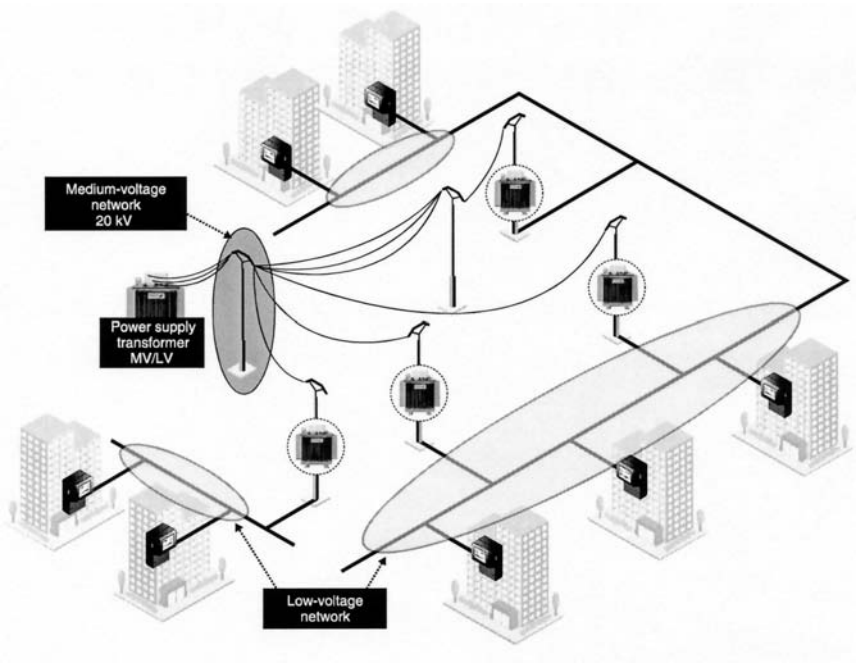

Figure 12.7 Example of a power line distribution system for a community

and the PLC infrastructure in collaboration with the operational teams of the local electrical utility.

The prime contractor team consists of electrical engineers for compliance with the safety rules and of telecom/network engineers for the use of the electrical infrastructure and the implementation of Internet services satisfying the residents' requirements.

PLC's Position Within the Network Architecture

The telecommunications networks can be considered as a large pyramid of networks comprising the following subnets (from top to bottom):

- *Very large networks.* Ensure very high throughput connections between towns and continents, usually using optical fiber, like Ebone or Europanet in Europe, Eassy for East Africa, SAT-3/WASC for the western part, and SEA-ME-WE-3 (from North Africa to India). Such network types cannot be built using PLC technologies.
- *Inter-POP backbones.* Connect the various very high throughput IP points of presence to the DataCenters of large cities. These optical fiber networks can be located between cities or in built-up areas. These backbones connect the points of presence to the exchanges (telephone exchange, cable TV, Satellite, WiMax, BLR, mesh, and so forth) of the Internet access providers. For the time being, PLC technologies cannot be used for building this type of network, but the throughputs provided by HomePlug AV and HomePlug BPL can be used for forming parts of this type of network in some cases.

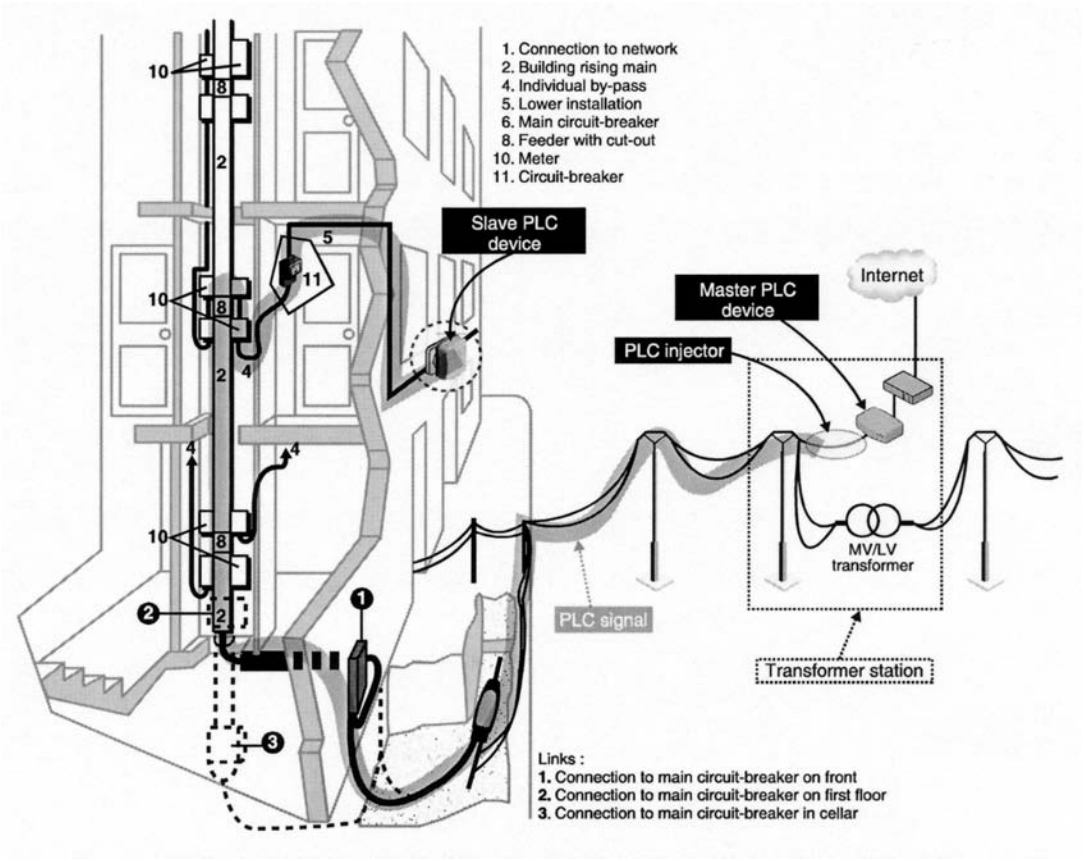

Figure 12.8 Topology and electrical devices in a building dense urban area

- *Distribution networks*. Used for connecting the exchanges of the Internet access providers and the subscribers to the Internet and to IP networks in general. These networks consists of all the media that can be used to reach the subscribers located at a few kilometers of the Internet access providers' exchanges. PLC technologies are undeniably ideal for distribution networks insofar as the topology of the electrical networks makes it possible to reach all the buildings and potentially each outlet of a community building.
- *Local area networks (LAN or interbuilding network)*. Usually Ethernet or Wi-Fi, they are likely to be replaced or completed by the PLC technology with non-negligible advantages (throughput, security, easy deployment, pervasive presence of outlets).

The issue with a community illustrated in this chapter is to build a distribution network using PLC technologies or according to a hybrid architecture combining several technologies making it possible to provide a high throughput Internet access to all the buildings of the community.

Figure 12.9 illustrates this telecommunications networks pyramid in which PLC technologies can place themselves at the level of LAN and distribution networks in the case of communities.

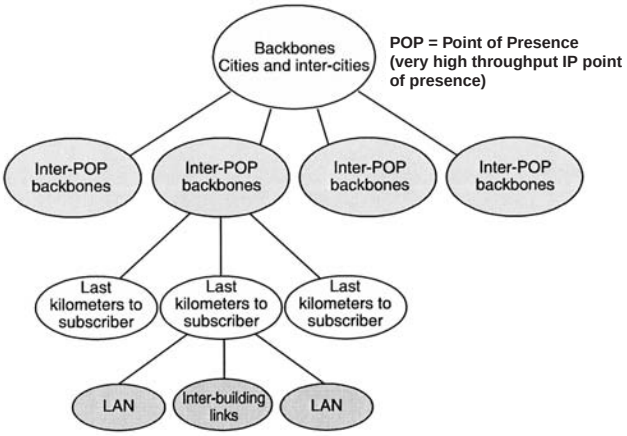

Figure 12.9 Telecommunications networks pyramid

Constraints of the Electrical Network for PLC Architecture

If the electrical network of a country supposedly not interconnected to its neighbors is examined, the main constraints influencing the architecture of a PLC network in a low voltage electrical network are the following:

- *Geographical area*. The network has different characteristics in a residential environment, in a corporate environment (generally with a higher meter density), or in an industrial environment (generally more demanding in terms of quality of service).
- *Number of meters per low voltage network*. High density difference between rural areas and dense office buildings areas.
- *Cable lengths*. Usually, the cable length to reach the subscribers varies from 50m (dense urban environment) to 300m (low density rural environment).
- *Network topology*. An electrical network consists of electrical wirings connecting the network transformers to the delivery points, the number of which varies according to the area under consideration.

However, it is important to be aware of the differences concerning the topology of the existing electrical networks in various countries, which implies new PLC constraints and can delete other constraints.

For example, in the USA, the housing outside big cities is very scattered and only a few meters are connected to a MV/LV transformer, whereas in France there are about 200 meters on average. In the case of the USA, it is understandable that the "transformer remoteness and number of customers sharing the resource" parameter is not as important as in Europe.

PLC Architecture

Using PLC technologies as a distribution network for a community in order to provide an Internet access requires a PLC network architecture different from the archi-

tecture that we have seen in Chapters 10 and 11 dedicated to home and corporate PLC networks.

The topology of the low voltage HTA electrical network of the community from the MV/LV transformer to the various building meters is a star topology. In addition, the distribution network requires an isolation between customers of the PLC network in order to prevent any interception of the data communications circulating between a PLC network customer and the Internet.

This implies a PLC architecture of the master-slave type in which the network master:

- Monitors, administers, and supervises the various network devices;
- Ensures the security and the confidentiality of the connections to the Internet and between each customer of the PLC network;
- Ensures the gateway functionality to other IP networks, and, more especially to the IP transit point available in the community (satellite, IP point of presence, optical fiber, BLR, WiMax, Mesh, and so forth).

Figure 12.10 illustrates an example of PLC architecture in a community from the MV/LV transformer to the various branches of the star network supplying the community buildings with electricity.

The key points of this architecture are the following:

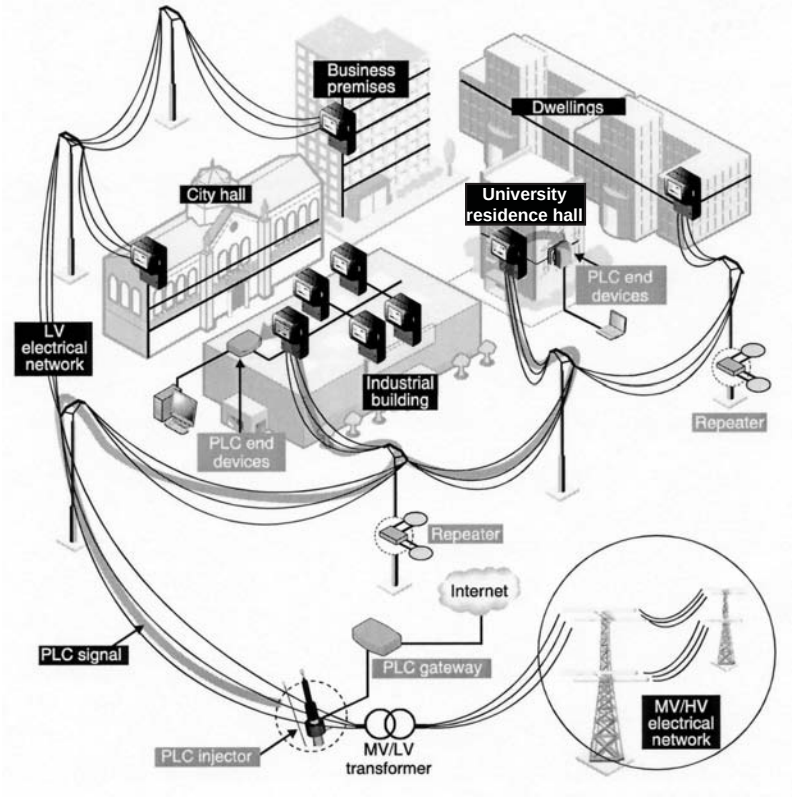

Figure 12.10 PLC architecture example for a community

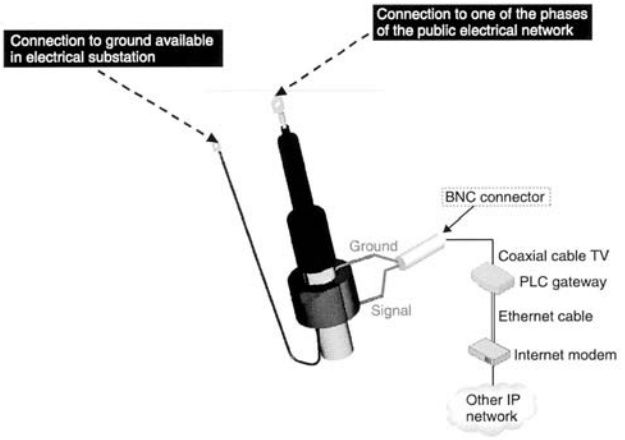

Figure 12.11 Example of connection for Eichhoff PLC injector

- PLC gateway used for the connection to other IP networks.
- PLC injectors used in the public electrical network installations as illustrated in Figure 12.11.
- PLC repeaters used for providing a continuous PLC signal over the entire cable length up to the subscriber, which can reach 200 to 300m. The advantage of the PLC network for local authorities is that the electrical network is much less subject to disturbance than a home or corporate network.
- Gateway located in the electrical substation where the MV/LV or HV/MV transformer is, which is used for injecting the PLC signal at the node of the star topology of the public electrical network.

This architecture of the PLC technology distribution network is in the end rather simple and generally without surprises, unlike that of a home or corporate network, for which the drawings of the electrical network are often lacking, which requires tests prior to installation.

In the case of the community network, the electrical utility has all the information concerning the electrical network (type of cables, cable length, number of subscribers on each branch of the electrical network, type of transformer, suitable position of the repeaters, etc.).

Issues in Electrical Networks

Installing a telecommunications device on a public electrical network is accompanied by a number of safety rules that must be complied with by all the parties intervening on the electrical network devices, in particular the operators and the electrical utility technical agents.

As far as the PLC networks are concerned, these rules are the following:

- Perfect isolation of the coupling and repetition devices;
- PLC device maintenance transparent to the operation of the electrical network;

- Intervention on PLC devices by authorized people.

The authorizations for interventions on an electrical network (deenergized, close or energized) are obtained via specific trainings and approvals by ad hoc bodies.

Table 12.1 lists the various authorizations for the various classes of technical parties intervening on an electrical network according to the work to be carried out.

The installation of telecommunications devices and more generally of electrical devices on the infrastructure of a public electrical network also raises a number of issues, in particular the following:

- Power supply of the PLC devices (installation of a power supply meter, billing of the PLC device power supply, and so forth).
- Nondisturbed operation of the electrical network and of its controlling devices.
- Possible identification of the low throughput PLC networks existing on the electrical network of the community electrical utility and of the location of these devices (electrical substation, pylon, and so forth).
- Possible coexistence of community PLC networks and of private home or corporate PLC networks. This coexistence between PLC networks and therefore between PLC technologies will be examined further in Chapter 13, which is dedicated to hybrid networks.

Choosing Equipment and Technologies

The choice of the PLC devices for a community network is particularly important insofar as the master-slave architecture required by this type of network makes it necessary to use a PLC technology incompatible with other technologies.

The Opera (Open PLC Research Alliance) project did not result in the development of a single PLC standard. Since the HomePlug alliance has not yet finalized in June 2008 the HomePlug BPL (Broadband PowerLine) version dedicated to the PLC networks of communities, the PLC technologies for the networks of communities are specific to each manufacturer, even if some of them use HomePlug as a basis to propose PLC products for the distribution networks of communities.

Therefore, it is important to compare the various technologies capable of satisfying the requirements of a master-slave architecture on the public electrical network. For this purpose, Table 12.2 summarizes the advantages and disadvantages of each PLC technology for a distribution network.

Table 12.1 Electrical Authorizations

AUTHORIZATION	*DEENERGIZED*		*CLOSENESS*		*ENERGIZED*	
	LV	*HV*	*LV*	*MV*	*LV*	*MV*
Non-electrician	B0	H0	BOV	HOV	—	—
Executing electrician	B1	H1	B1V	H1V	B1T	H1T
Work manager	B2	H2	B2V	H2V	B2T	H2T

Table 12.2 Advantages and Disadvantages of PLC Technologies for a Distribution Network

PLC SERVICE TECHNOLOGY	*DEVICE AND FUNCTIONALITY*	*ADVANTAGES*	*DISADVANTAGES*
Main.net	–CuPLUS master –RpPLUS repeater –NtPLUS slave	–Proven technology in various PLC projects –Good range of the PLC signal –Supervision tool (NmPLUS)	–Technology a bit obsolete
Spidcom	–Head-end master –Repeater –CPE slave	–Possible advanced configuration (notching, power spectral density, and so forth) –Strong engineering support –SPiDMonitor tool for administration/ supervision –224-Mbit/s throughput at PHY level	–Few deployments in France –Complex administration
DS2	–HE master –Slave of the apartment building type HG –Slave of the CPE apartment type	–Stable throughput over public networks –Simple management interface by HTTP –OMS-PLC tool for administration/ supervision –Product integration by Corinex equipment vendor	–Not compatible with HomePlug products
Ascom	–Master –Slave	–Easy Telnet interface –Easy software update	–Low throughput –Obsolete technology

The information in this table is only given as an indication but it should enable designers to choose the PLC technology best suited to the community specifications.

Supervision of the PLC Distribution Network

In the same manner as corporate PLC networks, the PLC distribution networks require a system for the supervision of the infrastructure devices.

The architecture of a PLC distribution network includes the following elements:

- PLC distribution network consisting of PLC devices in the master-slave mode and using the public electrical network up to the final subscriber.
- Connection of the PLC distribution network to other Internet constituent IP networks (via "peering" agreements) or directly to the Internet via an Internet access provider.
- NOC (Network Operation Center), central station where the stations supervising the various PLC distribution networks are grouped; these are used for checking the status of the network constituent PLC devices by means in particular of GPS mapping functionalities used for giving the position of each device.

Figure 12.12 illustrates an example of PLC distribution network architecture implementing VPN tunnels connecting the NOC to the PLC gateways existing in the electrical substations with links dedicated to the supervision of the network head devices.

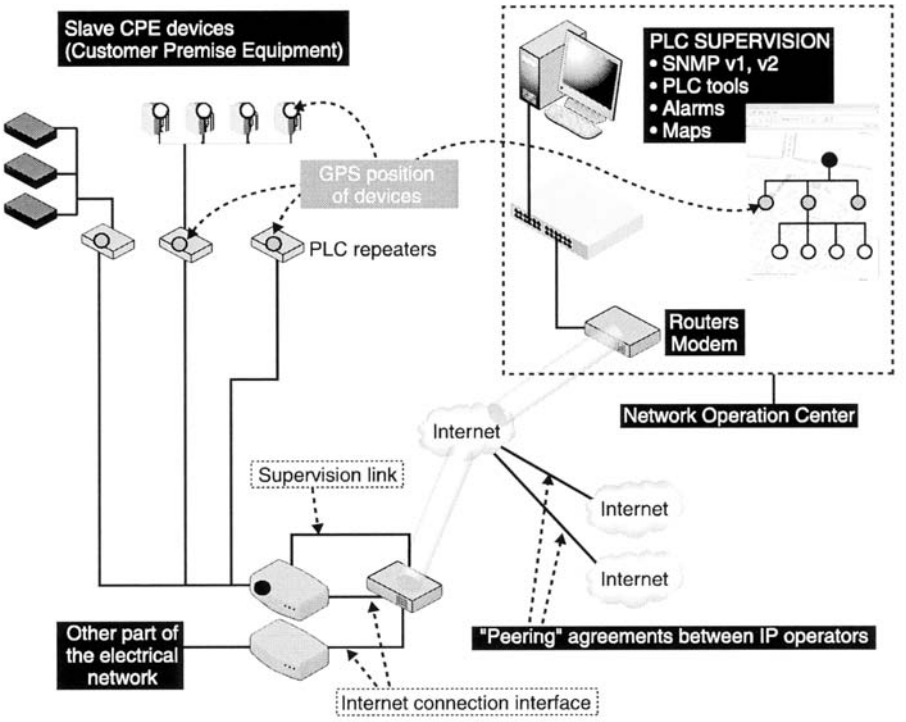

Figure 12.12 PLC distribution network supervision architecture

All the infrastructure devices can be supervised with the SNMP or TR-069 protocols using tools used for retrieving information (throughputs, status of the interfaces, temperatures, binary error rate, and so forth) and to trigger threshold alarms. The HP OpenView tool, for example, is used for centralizing the fed back SNMP data.

For the purely PLC parameters of the network devices, it is necessary to use tools specific to each deployed technology. For example, the DS2 products have the OMS-PLC tool developed by the Dynamic Consulting International company used for managing the supervision of a DS2 technology distribution network.

Configuring the Network

As we have seen, various technologies can be used to build a PLC distribution network; it is up to the prime contractor team to choose the technology best suited to the architecture requirements.

The example of a complete architecture for distribution network of a community illustrated in Figure 12.13 includes the following elements:

- IP networks upstream of the PLC network with the DataCenter, which groups authentication, address, and name servers; and the NOC, which deals with the supervision and administration of remote networks, like PLC distribution networks.

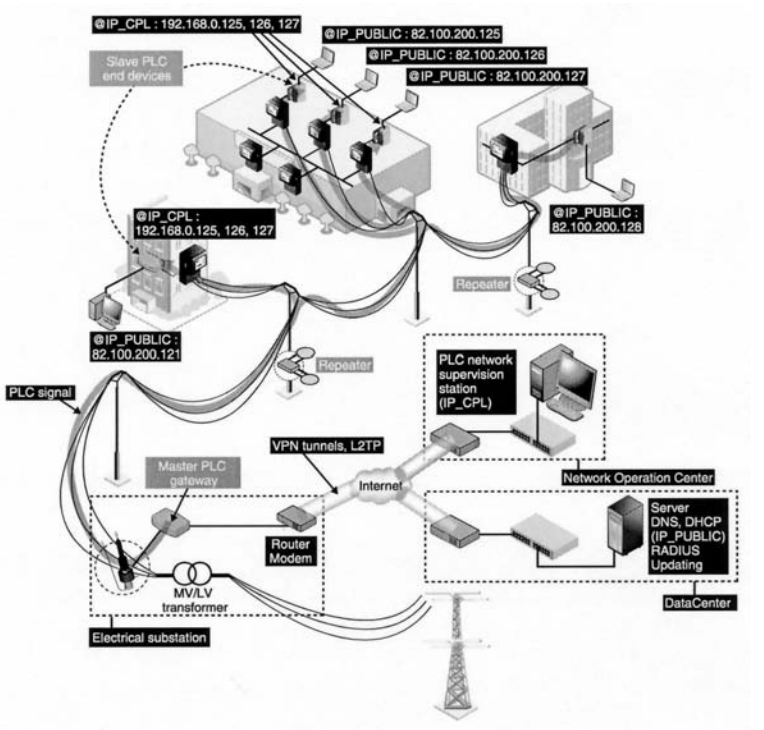

Figure 12.13 PLC distribution network architecture example

- PLC distribution network, with the master PLC gateway or gateways at the electrical substation (hosting the MV/LV transformer, the repeaters and the slave PLC devices (CPE)). The slave devices connect to the master device and are accessible via their IP addresses, which are in a private IP addressing plane different from that of public IP addresses delivered to the community subscribers.
- PLC injectors, which are used for connecting the PLC devices to the LV or MV public electrical networks at the electrical substation or to a point of an electrical pylon close to the final subscribers.

Since the configuration of all the devices for all the technologies cannot, of course, be given, we merely indicate the main parameters to be configured for each type of device of the distribution network infrastructure in Table 12.3.

GPS Position of Distribution Network Infrastructure PLC Devices

To optimize the supervision and the management of maintenance interventions on devices of the electrical network, each device can be spotted with its GPS position. This GPS position is also used for easily positioning the architecture components on a mapping available in the NOC (Network Operation Center) supervision tools.

Some products are used for configuring this position for each device via the HTTP interface of the distribution network master device, as illustrated by Figure 12.14.

Table 12.3 Parameters to Be Configured for Each Type of Device of the PLC Infrastructure of the Distribution Network

INFRASTRUCTURE DEVICE TYPE	*PARAMETER TO BE CONFIGURED*
Master	–Internet connection parameters –List of authorized slave devices –Filtering of MAC and IP addresses –Confidentiality of slave devices between themselves –Configuration of authentication servers (RADIUS, PPP, and so forth) –NAT and firewall for management interfaces
Repeater	–Segmentation of PLC network parts –PLC network keys –Physical or logical repetition
Slave	–PLC network keys –Authentication to the master device –IP PCL addressing for management/supervision –Management of priorities (QoS) and IP service classes (voice, data, video)

For this purpose, it is necessary to connect to the HTTP configuration interface of the products via VPN tunnels between the NOC and the PLC infrastructure devices used for viewing the NOC and the PLC network in the same local area network with a common addressing plane. For example, in Figure 12.14, the supervision station is in 192.168.1.10 and the PLC network is in 192.168.1.251.

Once connected to the interface, as illustrated in Figure 12.15, just select the desired device in the Source menu of the menu bar (slave devices or repeaters; these devices are spotted with their MAC address at the interface level).

Examples of Small, Medium, and Large-Scale PLC Networks

Several deployments of PLC networks over the electrical networks of communities have been experimented with in the last years.

These developments have enabled operators' research and development centers to carry out in situ tests on their technology on real network and subscriber cases. Communities supported by alternative operators, electrical utilities, and so forth have then prepared the first Internet subscription offers via PLC.

Other advances were made in the United States, in Spain, and in Switzerland where distribution PLC networks were deployed in entire cities. Lastly, China has deployed PLC networks with the FibrLink operator for tens of thousands of people living in new buildings.

The recent takeover of Current Technologies by Google shows that, for some major Internet players, the PLC networks represent a distribution technology with promising developments.

Small-Scale PLC Networks

Within the framework of its missions, the EDF research and development department deployed a PLC distribution network in 2002 in the commune of Courbevoie

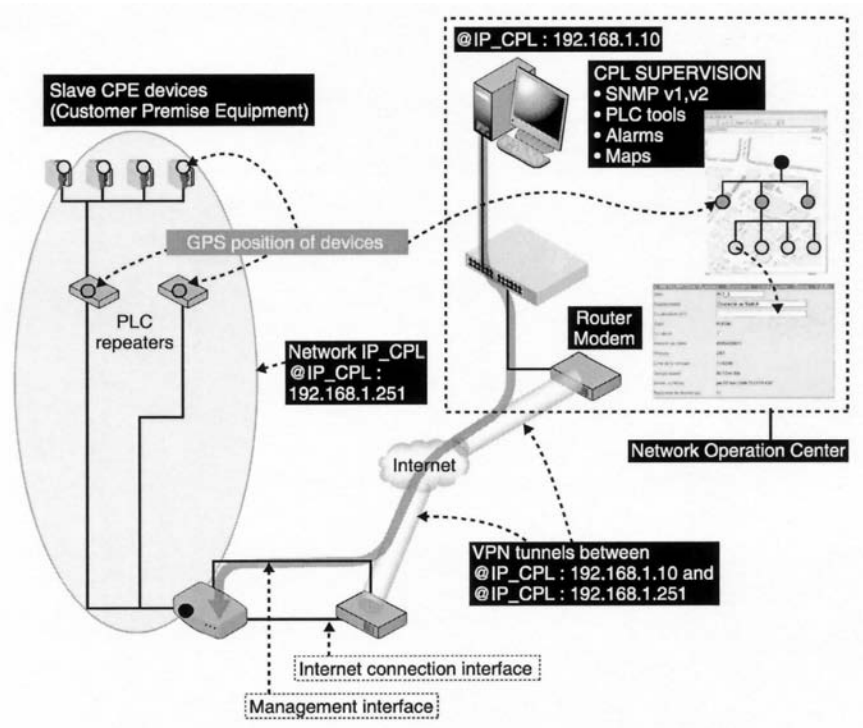

Figure 12.14 PLC device configuration architecture for GPS positioning of the distribution network devices

(France), with the support of the Tiscali Internet access provider for the Internet connection.

This distribution network was intended to test the quality of an Internet access over the EDF low voltage distribution network in a dense urban environment (star electrical network topology of the tree type).

The architecture of this infrastructure consisted of a very high throughput Internet access with an optical fiber at the local electrical substation that supplied between 100 and 200 EDF subscribers.

At the electrical substation, the PLC devices were used for injecting the PLC signal in the electrical wirings starting from the transformer and serving the apartments of the various local buildings. These electrical substation PLC devices were masters.

The slave PLC devices connected to the PLC network were located in the apartments. They had the suitable logical authorizations to recover the Internet signal originating from the Tiscali Internet access provider. This Internet access provider managed the users' authentications and the assignment of IP addresses to each customer of the PLC distribution network.

Medium-Scale PLC Networks

Within the framework of the digital gap reduction policy concerning high throughput Internet access in a rural environment, the Seine-et-Marne regional council (France) has deployed satellite, PLC, and Wi-Fi network technologies in the communes of Villeneuve-Saint-Denis and Villeneuve-le-Comte.

The deployment of PLC distribution networks has enabled the introduction of high throughput in "white" areas not served by ADSL offers. So, these two communes could have access to high throughput Internet from a point of presence close to the communes via a complete PLC architecture.

Large-Scale PLC Networks

Outside France, large-scale PLC distribution networks have been deployed in Spain (Saragossa and Barcelona) by the DS2 company and in the United States by Current Technologies, which has deployed PLC networks in the states of Maryland and Texas for a 4-Mbit/s symmetrical Internet access offer potentially aimed at two million people.

Fribourg (Switzerland) was among the first cities to deploy a PLC distribution network with the Ascom technology in 2001 with the Swisscom Internet access provider.

In France, one of the major PLC distribution network projects was supported by Sipperec, an administrative collectivity in the energy and communications field in the Île-de-France department.

Example of Deployed PLC Networks

Table 12.4 gives a wide range of examples of current and past PLC deployments worldwide.

Another European example is located in Germany with the company PPC.

In Germany around 10,000 end users are already using commercial Internet services over LV-PLC. Eighty-five percent of the end customers are using the PLC technology of Power Plus Communications AG (PPC). This technology is based on the PLC System of Main.net Ltd. (Israel). PPC is the PLC system integrator for Powerline equipment and on March 2005 installed, for a number of operators, several commercial and test installations all over Germany (103 MV PLC links).

In Germany, medium voltage powerline will be used in most cases as the backbone in the LV PLC network for substations, which have no direct connection to the fiber backbone.

Eighty percent of the lines are used as the backbone for an installed LV PLC system and 20% as rented or leased lines for professional industrial customers. One hundred and one of the total lines are realized with different types of capacitive coupling devices of PPC. In two test installations, inductive couplers of Eichhoff are installed.

PPC has equipped a wide spectrum of MV cells with PLC equipment. The MV cells diversify in voltage range and insulation of the cell itself. The voltage range varied from 6 to 30 kV. Figure 12.16 shows typical MV PLC installations in Germany for air and gas insulated (SF6) cells equipped with capacitive couplers.

Figure 12.17 shows another typical capacitive coupling device installation on an MV cell.

The maximum throughput is 3 to 5 Mbit/s, depending on line condition in the PPC deployment in Germany.

Table 12.4 Examples of Large-Scale PLC Networks Deployments Worldwide

DEPLOYMENT AREAS	*DEPLOYMENT COUNTRY*	*PLC OPERATORS*	*COMMENTS*
America	United States	Amperion	Cap Girardeau, MO
	United States	Current Technologies	HomePlug 1.0 Turbo, AV technology
	Brazil	Light	Low bit rate applications
Europe	Germany	EnBW	Based on ASCOM Technologies in the Ellwangen area
	Spain	Iberdrola	Based on DS2 technologies
	Denmark	PowerNet	Complementary to the Wi-Fi deployments
	France	TLIC	Based on the MECELEC network
	Germany	PPC	Main.net technology
	Spain	Epresa	Teleservice applications
	Spain	Endesa	Based on the DS2 technologies
	Russia (Moscow, Novgorod & Krasnodar)	Electro-com	Broadband Internet access, telephone, and television services for 35,000 customers
	Hungary (Budapest)	23Vnet	High speed broadband test on 100+ customers
Africa	Niger	Electrical operators	Tests in several cities
	Algeria	Sonelgas	Tests in schools, universities, hospitals
	Egypt (Alexandria, Fayed, Tanta)	Engineering Office for Integrated Projects, Corinex	Automatic Meter Reading on 70,000 customers
	South Africa (Pretoria)	Internet Access Solutions	Broadband internet access for 5,000 customers
Asia	China	FibrLink	50k test users
	Japan	Panasonic	In-house applications with NTT Docomo

As far as the United States is concerned, a good example is given by Current Technology.

In the USA, Current Technology deployed at the end of 2006, a BPL offer with TXU aimed at two million potential customers: this is a symmetrical 4 Mbits/s offer with VoIP for 45€ (see Figure 12.18).

The installation on a pylon consists of a device based on the HomePlug (1.0 or Turbo) product. The brand of the HomePlug products used by Current is AsokaUSA.

The installation is fitted with capacitive couplers, cut-off breakers, and fuses.

As far as the "BPL gateway" is concerned, it comprises a coaxial input (or optical fibers) and has router functions (QoS of VoIP flows + Authentication [IP filter] + PLC gateway).

HomePlug Turbo allows several keys (up to 24) and therefore allows the creation of several PLC logical networks.

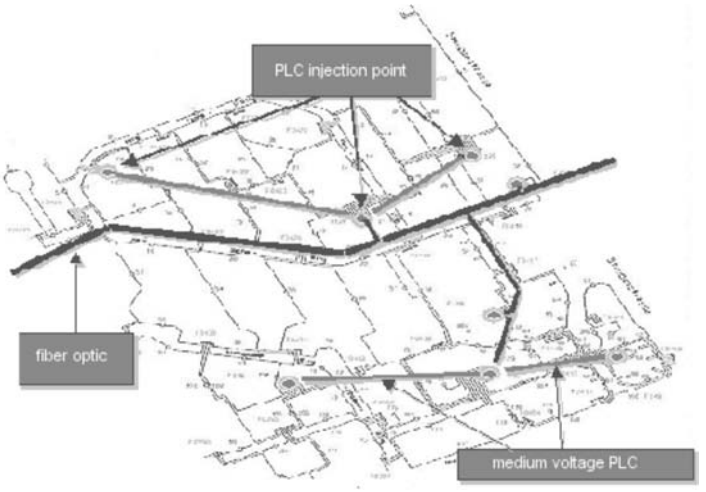

Figure 12.15 APPC PLC deployment architecture (Source CIGRE)

Figure 12.16 Example of capacitive coupling in air insulated MV cells (Source CIGRE)

Current Technologies has developed a repeater-amplifier product at the level of the physical layer that is used for reamplifying the PLC signal over the MV and LV lines without losing the bandwidth, like in the case of PLC repeaters operating on the MAC layer.

Current Technologies proposes to use the Internet access via PLC with the following configuration, for example:

- Bedroom: IP camera with IP flow from one room to another one;
- Living room: streaming video of an MPEG 4 flow (Windows Media 9 – 1.5Mbits/s encoder) from a video server;
- Office: PC + IP printer + Switch + Customer PLC devices.

Figure 12.17 Example of capacitive coupling in gas insulated MV cells (Source CIGRE)

Figure 12.18 Installation of a Current PLC gateway on a pylon (source Michel Goldberg)

Current proposes a system for collecting meter information over the MV and LV network. This information relates to the various electrical parameters available on the network (kVA, kWh, leakage currents, and so forth) via an HTTPS centralized interface at the disposal of the utilities.

This interface is used for displaying information on:

- A transformer (transformer load, historical report, and so forth);
- A meter (historical report, voltage, defaults, and so forth).

The interface can be operated with the GIS (Geographical Information Systems) of the utility. Therefore, the data of a transformer or meter can be displayed from the map of the area in question via this interface. The interface is also used for displaying defects on the electrical network according to the alarms fed back by the meters and the measuring instruments.

For Current Technology PLC/BPL is not the core business of the utilities and orients its business policy to the utilities by alleging that BPL can represent a source of income enabling the implementation of services of the AMR type (automatic meter reading and "intelligent powerGrid").

CHAPTER 13

Hybrid PLC

The recent developments of computer communication media have multiplied the network media (wired Ethernet, Wi-Fi, PLC, optical fiber, cable TV, and so forth) providing the suitable throughputs, coverage, and transit time to new generation applications.

Since none of these media offers by itself the ideal capacities, hybrid networks appeared in order to make the best use of these technologies. However, a good knowledge of them is necessary in order to optimize the architecture and the configuration of these new networks.

Nowadays, the wired Ethernet networks are those that are the most expensive, in particular because of the wiring-related work. However, they are still those providing the best performance and a guaranteed service close to 100%. When such networks cannot be built, it can turn out to be interesting to use complementary technologies as a basis.

This chapter aims at highlighting the interest of the current PLC technologies compared with other network technologies. With the emergence of the HomePlug AV specification, the PLC technologies add to the PLC advantages (easy deployment, low cost, open-endedness, security) and global performance capable of competing with these other technologies.

Coexistence of Multiple Networks

The coexistence of network technologies, whether wired or wireless, creates disturbance. For example, the propagation of PLC signals over the electrical wirings emits an electromagnetic field likely to disturb not only the other communication systems, like radio networks, but also the various PLC technologies themselves.

Since one of the major developments with regard to the network coexistence is precisely the juxtaposition of PLC and Wi-Fi, it is important to understand and control these disturbances.

PLC Technologies Between Themselves

As we have seen throughout this book, there is no IEEE PLC standard as yet. As a result, a number of PLC technologies coexist on the public and private electrical networks.

Figure 13.1 illustrates a house in which the three following PLC technologies coexist:

- PLC community distribution to provide an access to the Internet;
- LAN for the broadcasting of video streams from the InternetBox to PLC devices close to the video terminals scattered in the house;
- LAN for the broadcasting of the IP telephone signal and house automation (remote controls, sensor information, and so forth) and domestic signals (baby phones, video surveillance, and so forth) in the house.

Since these three technologies are high-throughput technologies, all of them operate in the 2 to 30 MHz frequency band, but with distinct techniques for gaining access to the medium and using the frequency band. Without any interoperability standard, these PLC technologies were concurrently developed without regard for their mutual coexistence.

The CEPCA (Consumer Electronics Powerline Communication Alliance) is currently working on the development of a guide on interoperability between PLC technologies that should allow optimized use of this frequency band.

CEPCA and Interoperability of PLC Technologies

Awaiting a PLC standard, the CEPCA has prepared a technical proposal in order to manage the coexistence of PLC technologies. This proposal is based on a CDCF (commonly distributed coordination function) used for managing the time and frequency spaces in a distributed way between the various technologies.

This distribution is based on the following elements:

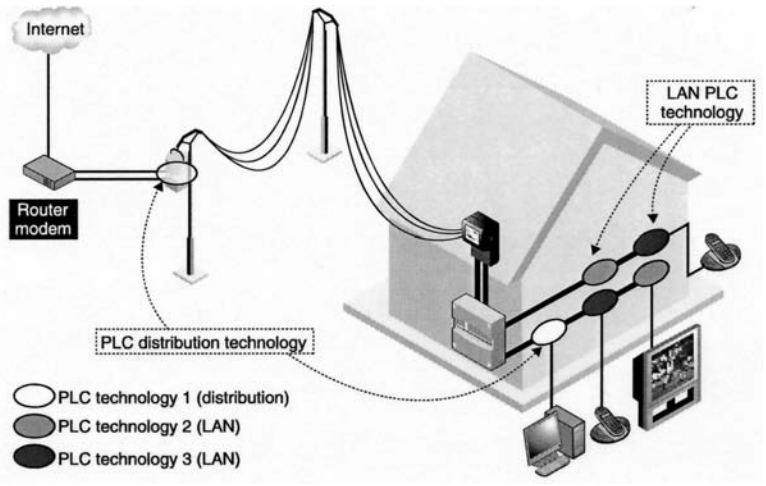

Figure 13.1 Coexistence of PLC technologies over the same electrical network

- Management of hybrid accesses between FDMA (frequency division multiple access) and TDMA (time division multiple access);
- Management of the QoS by a TDMA time space system, like in HomePlug AV for HD video applications.

As illustrated by Figure 13.2, these two principles should make it possible to avoid mutual interference and optimize the use of the common communication medium.

The main problem relating to the coexistence of PLC technologies comes from the fact that the use of the frequency band is not standardized. This results in a reduced available bandwidth for each technology. Data communications are still operational but in degraded, even highly degraded, modes that are detrimental to the routing of the provided services to the upper layers (IP, TCP, and so forth) and prevent the good operation of the applications.

In the same way as the presence of too many PLC devices on the same electrical network must be avoided (limited to 16 devices in the HomePlug 1.0 and Turbo specifications), it is necessary to avoid the implementation of several PLC technologies on the same electrical network (HomePlug, DS2, Spidcom, and so forth).

The CEPCA alliance proposals are close to those implemented in HomePlug AV, which provides a mechanism for the coexistence of HomePlug 1.0, Turbo, and AV networks with a TDMA time space allocation scheme (see Chapters 3 and 5).

Figure 13.3 diagrammatically illustrates this coexistence system, in which some time periods are allocated to data exchanges between HomePlug 1.0 devices and other periods to exchanges between the devices of other HomePlug specifications.

This type of intelligent management of the coexistence of devices from various HomePlug technologies should be extended to other technologies with the expected development of an IEEE standard.

As indicated in Table 13.1, the various HomePlug specification developments always attempted to promote interoperability and therefore open-endedness of PLC networks. On the other hand, the other PLC technologies are neither interoperable with HomePlug nor between themselves, which highly restricts the open-endedness of these networks.

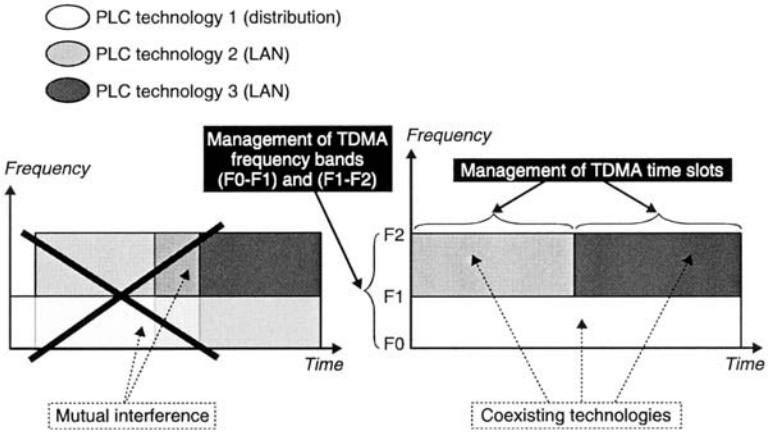

Figure 13.2 Proposal for the management of mutual interference between PLC technologies

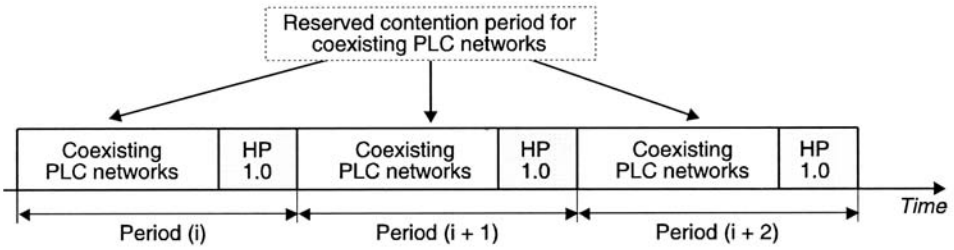

Figure 13.3 Management of coexisting HomePlug PLC networks with the HomePlug AV specification

Table 13.1 Interoperability Between PLC Technologies

PLC TECHNOLOGY A		*PLC TECHNOLOGY B*						
		HomePlug					DS2	Spidcom
		1.0, Turbo	AV	Oxance	BPL	CC		
HomePlug	1.0, Turbo							
	AV							
	Oxance							
	BPL							
	CC							
DS2 AV200								
Spidcom								

Coexistence of PLC and Wi-Fi

There are no problems with coexisting PLC and Wi-Fi technologies since different frequency bands are used, with PLC operating in the 1-MHz to 30-MHz frequency band and the various IEEE 802.11 standards in the 2.4-GHz and 5-GHz frequency band.

In terms of architecture, there are no problems with the coexisting technologies either, which makes it possible to use the best of both technologies. Therefore, many PLC/Wi-Fi hybrid devices should appear to build architectures combining a PLC backbone and IP distribution of the radio type with Wi-Fi.

The Lite-On company has already announced the imminent release of a PLC/Wi-Fi device of the bulb type for a ceiling light socket. This device will make it possible to use the electrical network that supplies the bulbs to convey the PLC signal while providing PLC functionalities and Wi-Fi access points to this new "intelligent" bulb generation.

Placing a Wi-Fi access point at the ceiling level for a room is ideal for optimum radio coverage.

Figure 13.4 illustrates an example of PLC/Wi-Fi architecture with an Internet access connected to a PLC gateway device broadcasting the PLC signal over the electrical network. This signal is recovered by PLC/Wi-Fi devices using their 802.11 radio interface to create Wi-Fi cells in the various rooms.

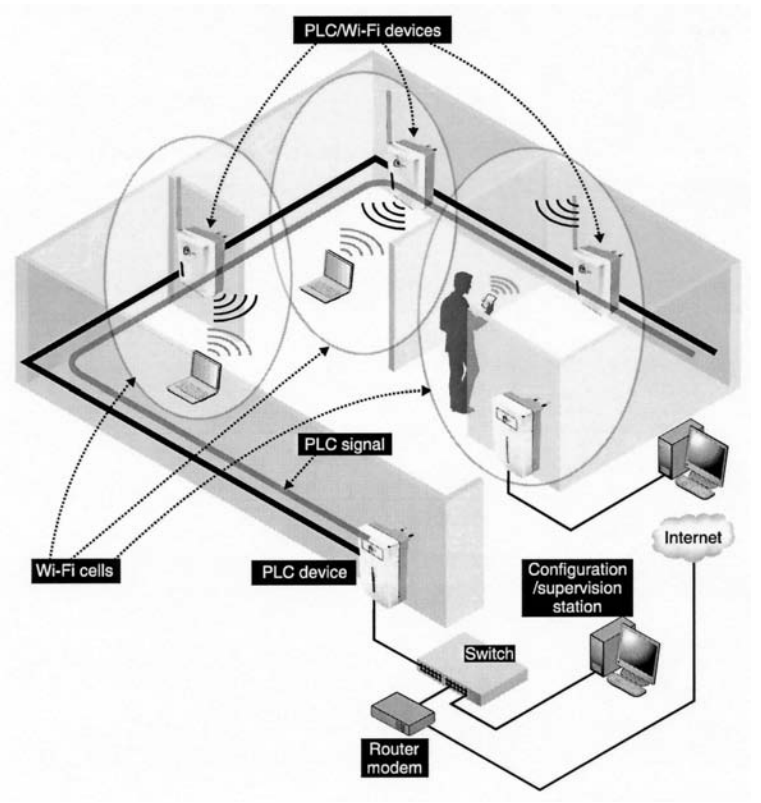

Figure 13.4 PLC/Wi-Fi hybrid architecture example

The NBG318S devices from Zyxel, illustrated in Figure 13.5, will be used to illustrate the configuration of such an architecture.

Zyxel proposes a router including a device fitted with an Ethernet PLC interface and a Wi-Fi interface with an outlet and an aerial for the IEEE 802.11 interface.

The configuration of this hybrid network requires access to the Wi-Fi device parameters. These parameters are configured via an HTTP interface at the Wi-Fi device level, as illustrated in Figure 13.6.

The address of the network configuration station is IP = 192.168.1.2 in the figure and the default address of the PLC/Wi-Fi device to be configured is 192.168.1.1. All you have to do is connect the Ethernet supervision station to the PLC device and open Internet Explorer at the 192.168.1.1 address.

The window illustrated in Figure 13.6 is then displayed. The default password is 1234.

After the connection, the HTML page illustrated in Figure 13.6 is displayed with the Wi-Fi access point default parameters. The security for this access point must then be configured.

In the Wireless LAN submenu of the Network menu, it is important to change the user name and the password for gaining access to the device administrator interface in order to avoid other people connected to the PLC network reaching the Wi-Fi network configuration.

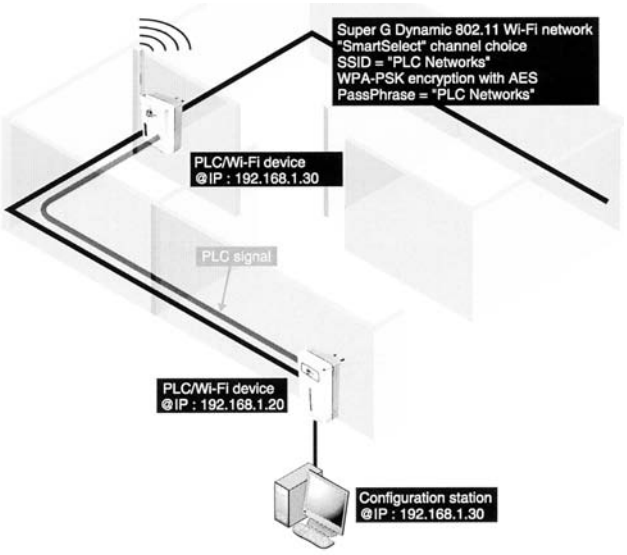

Figure 13.5 Configuration of PLC/Wi-Fi devices

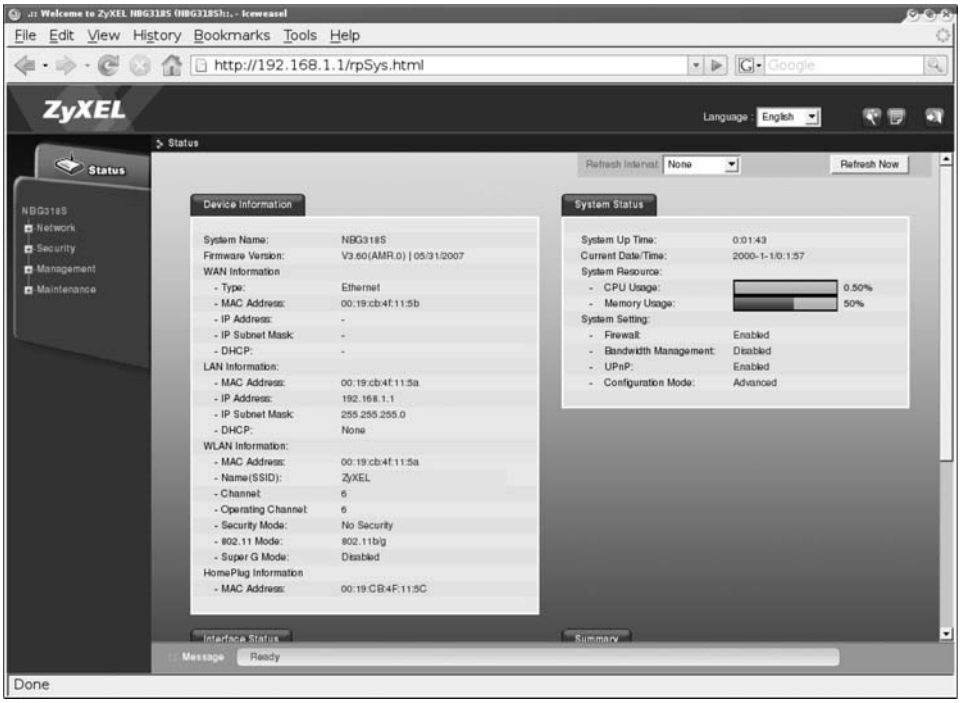

Figure 13.6 Connection to the PLC device used as a Wi-Fi access point

The next configuration step concerns the parameters specific to the Wi-Fi network and to its security. First, an SSID (i.e., a Wi-Fi network name) must be chosen so that the clients wanting to connect recognize it. PLC Networks is chosen here as illustrated in Figure 13.7.

A channel (from 1 to 13) can then be selected in the 2.4-GHz band.

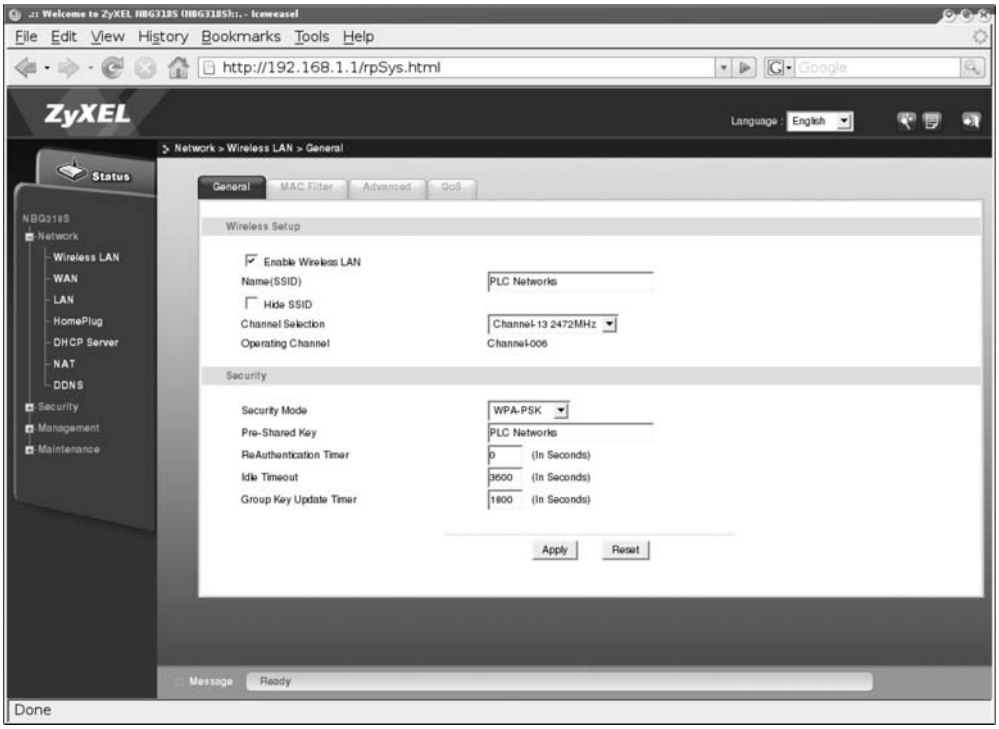

Figure 13.7 Configuring the Wi-Fi access point properties

Choosing the IEEE 802.11 Mode

When the network is configured in the "802.11 Super G dynamic" mode, it is important to make sure that all the 802.11 clients connecting to the network support this mode. If this is not the case, choosing the 802.11b or 802.11g modes supported by most current Wi-Fi terminals is preferable.

Once the 802.11 network mode is configured, we can proceed with the parameterization of the Wi-Fi network security, which is one of the weaknesses of Wi-Fi networks.

Insofar as the PLC network is made secure and physically difficult to access, a satisfactory security level can be maintained for the entire hybrid network. In our example, the Wireless Security submenu of the System Configuration menu is used for choosing the WPA-PSK mode with encryption of the AES type key (however, this mode must be supported by the client Wi-Fi boards, which is generally the case with recent boards) by indicating the encryption phrase (in this case, PLC Networks, as illustrated in Figure 13.7).

The global configuration of the Wi-Fi network is over. We can proceed with the configuration of the PLC network and of its parameters. As illustrated in Figure 13.8, the Homeplug submenu of the Network menu is used for gaining access to a page for configuring the HomePlug AV PLC parameters like the network name: Public (default key with unchanged value HomePlugAV) or Private by configuring a new NEK key for the PLC logical network consisting of this device and other PLC devices existing on the electrical network.

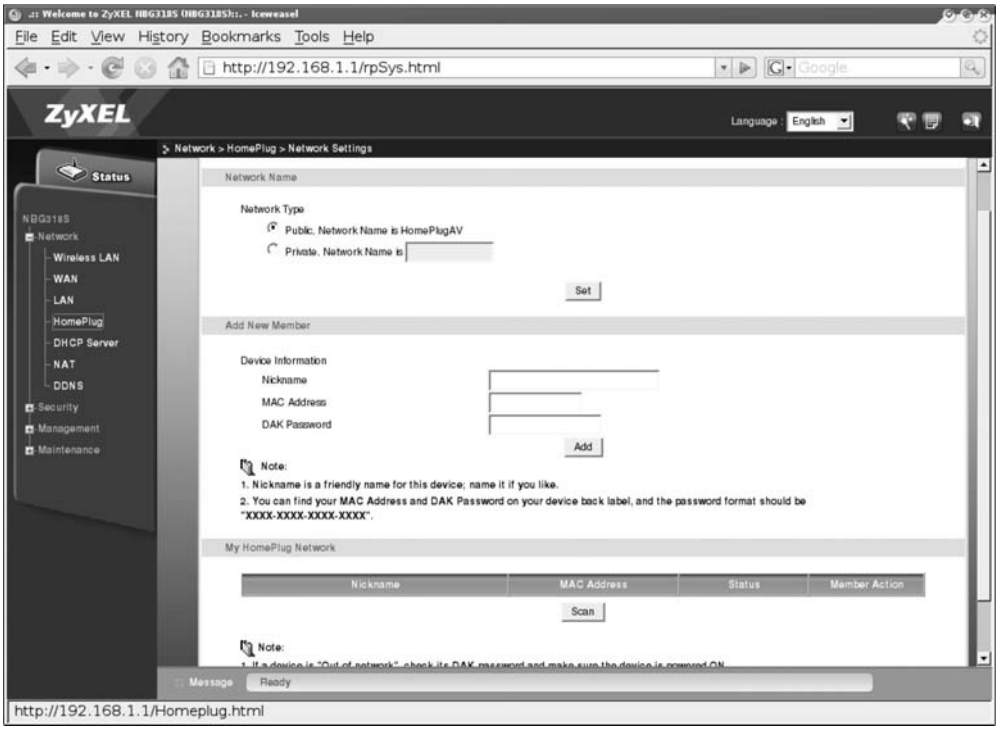

Figure 13.8 Configuring the parameters of the HomePlug AV PLC network

The network PLC devices must also be named in order to have a better readability of the network with respect to the MAC addresses of each device. In this case, the default name of the associated device is Example 1. Figure 13.8 shows the association of a new device and Figure 13.9 indicates the result of this association when the HTML page is refreshed.

Once all the PLC devices are associated with the HomePlug AV network, it is possible to choose the routing mode between the Wi-Fi and PLC interfaces. This interface acts as a gateway for the other one, which allows bridging between these two technologies.

Finally, the WAN interface used for the connection to the Internet gateway or to a router for access to another IP network from this subnet, as illustrated in Figure 13.10, can be chosen.

This configuration example shows that a PLC/Wi-Fi hybrid network architecture including integrated devices allows the easy and quick deployment of a network with optimum performance using the electrical network as the Ethernet backbone and the PLC/Wi-Fi devices on outlets as the distribution network with complete radio coverage.

In this way, the coexistence of PLC and Wi-Fi is both logical and natural to provide mobility in a domestic as well as professional background.

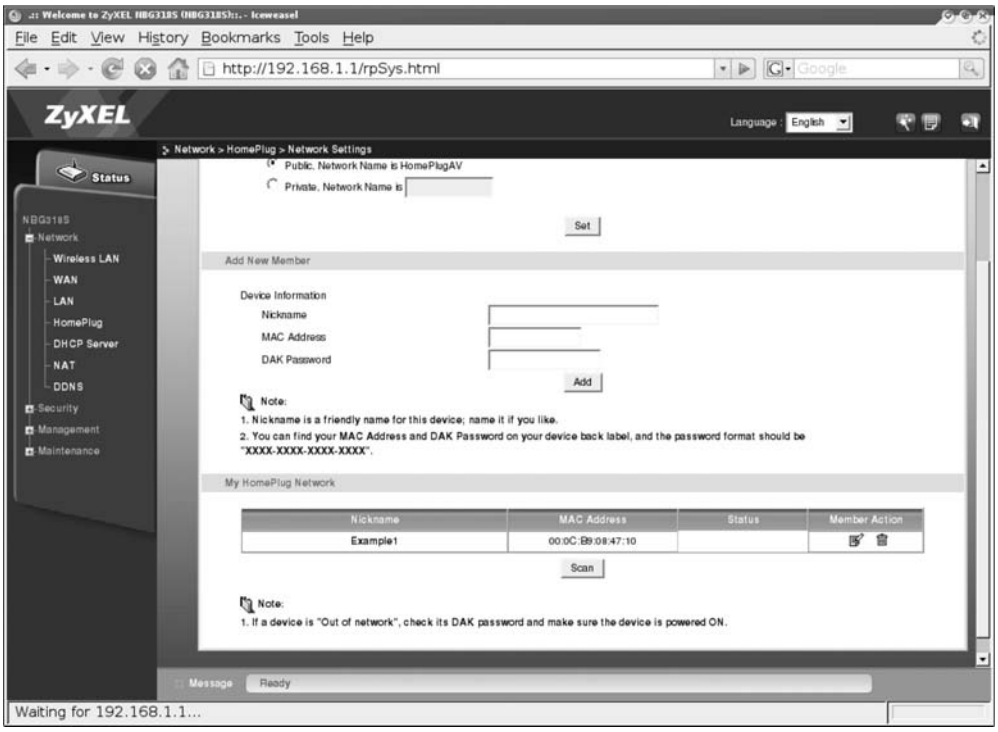

Figure 13.9 Confirmed association of a new PLC device on the network

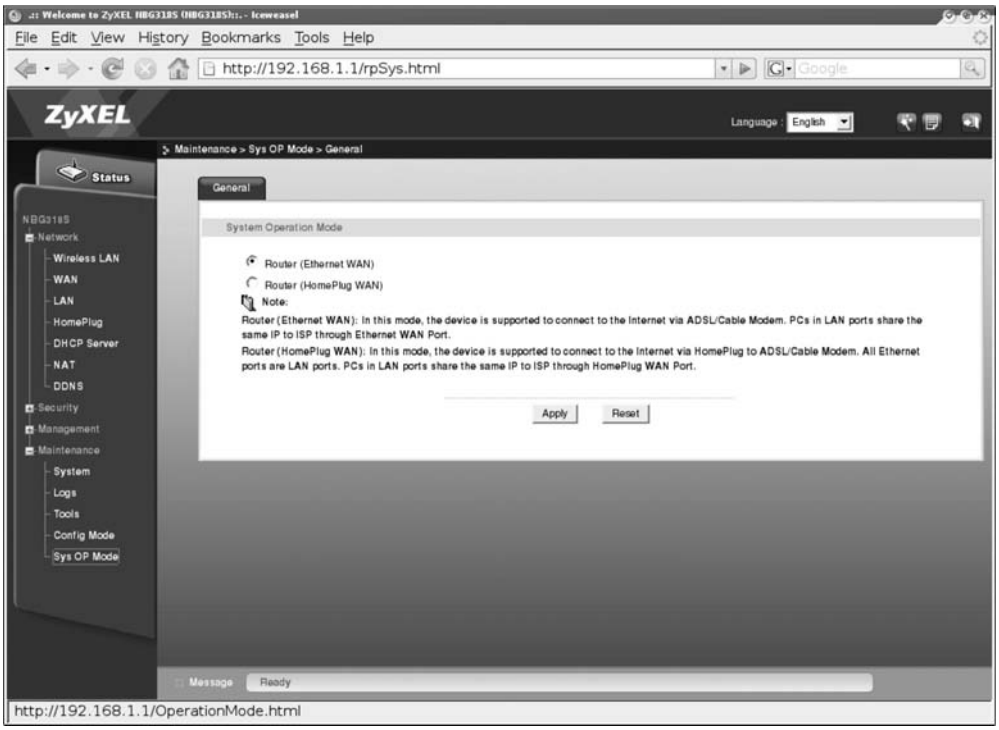

Figure 13.10 Configuring the WAN interface choice

Coexistence of PLC and Wired Ethernet

The coexistence of PLC and wired networks (Ethernet cable, optical fiber, cable TV, telephone cable, and so forth) does not generate disturbances since all the frequency bands used by these technologies are outside of the PLC frequency bands.

Only the VDSL distribution technology, which will allow reaching throughputs of several tens or so of megabits per second over copper telephone cables, will use the 138-kHz to 12-MHz frequency band. Therefore, it is likely to be subjected to potential interference, since PLC technologies use the 2- to 30-MHz band emitting an electromagnetic noise around the electrical wirings, which can reach 70 to 80 dBμV ("quasipeak" value).

Figure 13.11 illustrates the various VDSL bands and the place of the PLC bands in this frequency space.

In the field of local area networks, there are no problems with coexisting PLC and wired technologies so that wired technologies are frequently used as backbones for PLC local area networks.

Advantages and Disadvantages of Network Technologies

To make a comparison between PLC technologies and other network technologies, Table 13.2 summarizes the main advantages and disadvantages of each of these technologies.

Some of them have developed to a large extent because they met requirements by providing functionalities not provided by other technologies (price, easy deployment, open-endedness, security, and so forth).

Optimizing Network Architectures

The multiplication of currently available network technologies makes it legitimate to look for the best of each technology in order to build an optimal network architecture.

For this purpose, it is important to analyze the specifications for the network to be implemented and to list the most important characteristics of the building to be equipped.

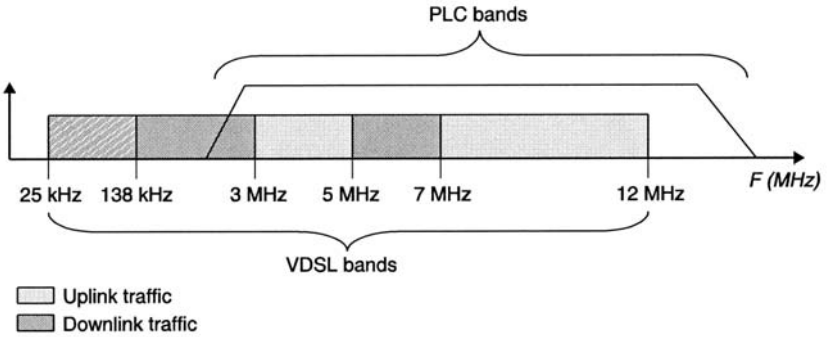

Figure 13.11 Potential interference between VDSL and PLC bands

Table 13.2 Comparison Between the Various Network Technologies

NETWORK TECHNOLOGY	*COST*	*DISADVANTAGES*	*ADVANTAGES*
Ethernet cable (CAT5 100baseT)	High	–Raceway –Cable cost	–Guaranteed QoS –Increased security (RJ-45 connector access control, filtering) –Guaranteed throughput –Power supply by PoE
Wi-Fi (IEEE 802.11g)	Average	–Radio coverage study –WPA and AES encryption implementation –Required RADIUS server –Non guaranteed QoS	–Network open-endedness –Mobility and handover –ToIP on Wi-Fi –Hybrid network with wired backbone
Cable TV	High if raceway	–Raceway –Potentially shared medium requiring authentication	–Possibility to use existing cables –Guaranteed QoS –Difficult access to physical medium
Optical fiber (plastic fiber)	High	–Raceway –Cost of active devices	–Very high throughput –Noise immunity –Ideal for wired backbone –Difficult access to physical medium
HomePlug Turbo PLC	Average	–Requires site and electrical network engineering study –Requires good knowledge of the electrical network –Difficult access for some device locations	–High useful throughput –Easy configuration –Network open-endedness –Possible temporary network –Medium security –Several VLAN on same electrical network
HomePlug AV PLC		–Requires good knowledge of the electrical hazards	–Useful throughput for HD video applications –Guaranteed QoS –Coexistence with other HomePlug 1.0 and Turbo devices –Compliance with electromagnetic immunities –Hybrid PLC/Wi-Fi networks
Telephone cable	High if raceway	–Public telephone cable belonging to France Télécom	–Use of existing cables –High and guaranteed throughput –Guaranteed QoS –Physical medium security

The network engineering study aims at identifying the following characteristics in particular:

- Structure of the buildings (size of the rooms, raceway possibilities, materials of the walls for radio transmission, and so forth);
- Existing networks (private telephone networks connecting several buildings of a site, cable TV networks, and so forth);
- Electrical network mapping and position of the circuit breaker panel;
- Expected network performance for applications (transit time, latency, jitter, and so forth);

- Open-endedness, removal requirements, temporary networks, test networks, and so forth;
- User groups and requirements of specific logical networks;
- Easy network deployment, configuration, and global supervision.

It is essential to specify these characteristics to build a network architecture that is both efficient and stable in time.

In the same manner as we have made a table in which the advantages and disadvantages of the various network technologies are compared, the optimum utilization conditions of each of these technologies are detailed in Table 13.3.

Example of an Optimized Architecture

We are going to take the example of the computer network of an installation with two buildings already fitted with private telephone lines starting from a local PABX to connect the two buildings.

Since these are multistory buildings, we want to implement user mobility in each room and between the two buildings. We assume that the rising mains are accessible and that they allow the passage of additional cables and easy installation of network devices.

A good knowledge of the electrical network of each story and of the entire building, if this is possible, is necessary for the installation of the PLC devices.

To satisfy these requirements and comply with these specifications, the hybrid architecture illustrated in Figure 13.12 consists of the following elements:

Table 13.3 Optimum Utilization Conditions of Network Technologies

NETWORK TECHNOLOGY	*OPTIMUM UTILIZATION CONDITION*
Ethernet cable	–Easy raceway (rising mains, other expected work, power supply by PoE, and so forth) –Optimum network architecture (star, ring, branches, and so forth)
Wi-Fi	–Efficient radio coverage –Good handover management between cells –Good security management
Cable TV	–Easy raceway –Easy existing medium access
Optical fiber	–Easy raceway –Active devices optimizing multiplexing –Good choice of optical mode and wavelengths
PLC	–Good knowledge of the electrical network –Hybrid network with wired backbone
Telephone cable	–Possibility to place devices close to PABX –Available point-to-point links

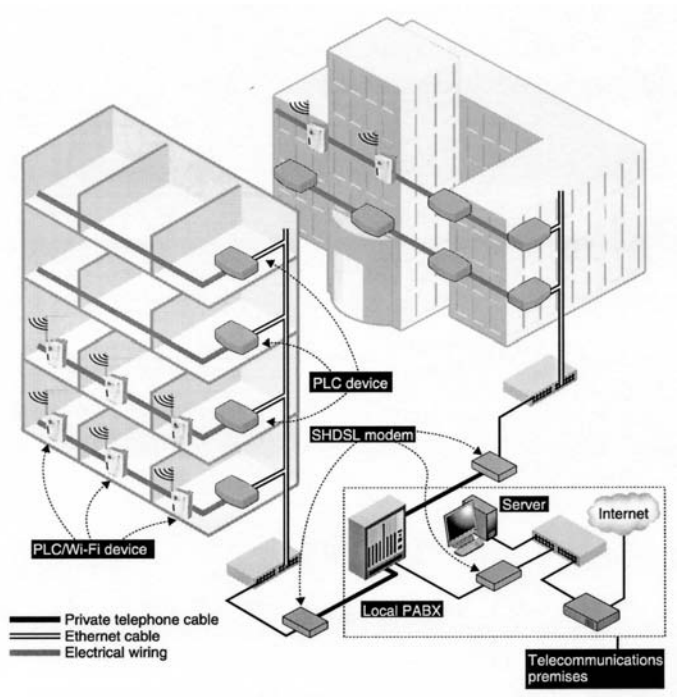

Figure 13.12 Example of optimized hybrid architecture

- IP links between the telecommunications premises and the buildings using SHDSL modems over twisted pair telephone cables;
- Ethernet backbone along the rising mains to supply each story with IP connection;
- PLC story network with a gateway device for each story connected to the Ethernet backbone;
- PLC/Wi-Fi hybrid device with an outlet in each room in order to ensure complete Wi-Fi coverage;
- Clients connected to the network either by means of IEEE 802.11 boards or use of PLC devices connected to the story PLC "gateways."

This architecture is just an example of a hybrid network. However, it makes optimal use of the constraints of the network installation site. Each of these constraints can turn into an advantage if the suitable network technology is chosen.

PLC and Wi-Fi, a Perfect Couple?

As indicated on several occasions in this book, there are many similarities between PLC and Wi-Fi technologies with the exception of the communication medium concerning the proposed throughputs, functionalities, or even device cost. Therefore, it was rather logical to notice that these two technologies get closer to allowing use of the electrical network as the Ethernet backbone and the Wi-Fi interfaces to connect the customers of the local area network.

An increasing number of manufacturers propose devices combining both technologies. The development of the latest standards will soon bring devices combining

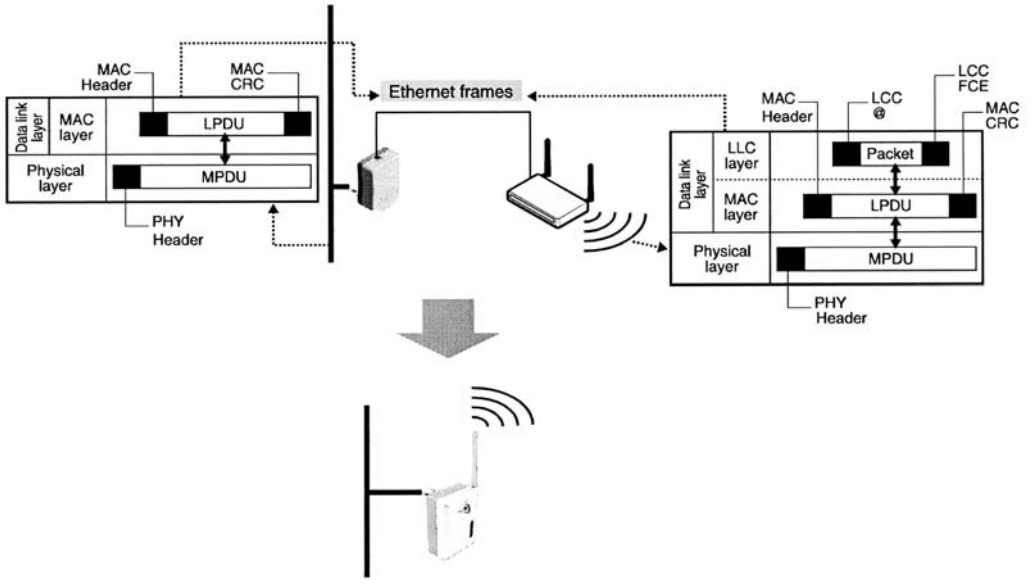

Figure 13.13 Optimized PLC/Wi-Fi devices

HomePlug AV and IEEE 802.11 Super G dynamic to market in order to provide better throughputs and the broadcasting of HD video streams.

Figure 13.13 illustrates the exchange of frames between a PLC device and a Wi-Fi device with an example of a PLC/Wi-Fi hybrid device below. The manufacturers are currently working on the optimization of the connections between PLC and radio interfaces in order to avoid frame encapsulation and de-encapsulation phases.

Resources

Web Sites

Standardizations Organizations

IEEE: http://www.ieee.org
http:// grouper.ieee.org/groups/1901/ for the PLC network working group
ETSI: http://www.etsi.org
IETF: http://www.ietf.org
Cenélec: http://www.cenelec.org
IEC and, namely, CISPR: http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirdet.p&progdb=db1&committee=CI&css_color=purple&number=CIS/I

PLC Technologies

HomePlug: http://www.homeplug.org
DS2: http://www.ds2.es
Spidcom: http://www.spidcom.com

Portals on PLC

CPL News: http://www.cpl-news.com
Powerline Communications: http://powerlinecommunications.net
PUA: http://pua-plc.com
PLC Forum: http://www.plcforum.org
CEPCA Alliance: http://www.cepca.org

Products

http://www.aceex.com
http://www.acer.com
http://www.amigo.com.tw/
http://artimi.com/
http://asokausa.com/

http://www.atlantisland.it/
http://bewan.com
http://www.billion-france.com/
http://cometlabs.com/
http://www.courantmultimedia.fr
http://www.connectland.net/
http://www.corinex.com
http://www.defidev.com/
http://www.devolo.com
http://www.dynamode.co.uk/
http://www.edimax.com/
http://eichhoff.de
http://www.gigafast.com
http://www.ilevo.com
http://www.jaht.com/
http://www.leacom.fr
http://www.linksys.com
http://www.Main.net-plc.com/
http://global.mitsubishielectric.com/bu/plc/
http://www.msi-computer.fr/
http://netgear.com/
http://www.niroda.com/
http://www.olitec.fr/
http://www.ovislink.fr
http://www.packardbell.fr
http://peabird.com
http://phonex.com
http://www.powernetsys.com
http://www.powertec.com.au
http://www.sagem.com
http://www.schneider-electric.fr
http://siemens.com
http://smc.com
http://www.stt.com.tw
www.sei.co.jp
http://www.telkonet.com
http://www.omenex.com
http://www.xeline.com
http://www.xnet.com.tw
http://www.yakumo.de
http://www.zyxel.fr

Low Bit Rate PLC Technologies

http://www.siconnect.com
http://www.itrancomm.com
http://www.arianecontrols.com

Books and Articles

DOSTERT (KLAUS), *Powerline Communications,* Prentice Hall, 2000

LEE (M. K.), NEWMAN (R. E.), LATCHMAN (H. A.), KATAR (S.), YONGE (L.), *HomePlug 1.0 Powerline Communication LANs—Protocol Description and Performance Results, version 5.4, 2000,* Wiley.

PAVLIDOU (F.-N.), LATCHMAN (H. A.), HAN VINCK (A. J.), NEWMAN (R. E.), "Powerline communications and applications," *International Journal of Communication Systems,* 2003, Wiley.

HRASNICA (H.), HAIDINE (A.), LEHNERT (R.), *Broadband Powerline Communications: Network Design,* 2004, Wiley.

About the Author

Xavier Carcelle earned an M.Sc. in EE from Ecole Normale Supérieure, France. He has held different positions in the industries of energy and telecommunications in France and in the United States. He worked for 6 years at Electricité de France, the largest electrical utility worldwide, as a telecommunications expert for PLC and wireless networks. In the United States, he worked as a software engineer on video compression algorithms for IP networks. He lectures in telecommunications at several universities in Paris and is a guest lecturer at the University of Florida. Xavier Carcelle is currently a member of the technical working group for IEEE 1901 PLC standardization body.

He currenly holds the position of CTO for the company OPENPATTERN, which is developing open hardware network routers.

Index

A

ACK response, 46, 47
Active repeaters, 145
Address classes, 212–213
AES (Advanced Encryption Standard), 65–66
AIFS (allocation interframe spacing), 41
Analogy with network hub, 25, 26
Antinoise filters, 147, 149
Applications, 107–124
  audio broadcasting, 118
  economic perspectives, 123–124
  file sharing, 116–117
  in industry, 121
  InternetBox, 119–121
  Internet connection sharing, 116
  in motor vehicles, 122–123
  multimedia, 114–115
  over coaxial cable, 122
  printer sharing, 116–117
  in public spaces, 122
  recreational, 118
  telephony over PLC, 108–114
  video surveillance, 118–119
  visioconferencing/videoconferencing, 114
  Wi-Fi network backbone, 119
Architecture, 15–29
  business PLC, 248–250, 256–257
  centralized mode, 37
  community PLC, 278–280
  DHCP, 239–245
  electrical networks, 15–24
  hotel PLC, 264–266, 268
  layered, 27–29
  master-slave mode, 126
  optimized, 304–308
  in peer-to-peer mode, 34, 130
  PSTN, 16
  with shared medium, 24–27
ARQ (automatic repeat process), 45–49
  acknowledgment frames, 46
  ACK response, 46, 47
  defined, 45
  FAIL response, 46, 48–49
  NACK response, 46, 48
  SACK response, 49
Ascom, 128, 129
AsokaUSA PowerManager, 188
Attacks
  brute force, 72
  decryption, 79–80
  dictionary, 72
  DoS, 71, 80
  PLC networks, 78–80
  on security holes, 72
  spoofing, 72
  virus, worm, Trojan horse, 72
Attenuation, 20–21, 165–167
  cable length and, 168
  for meter and circuit breakers, 20
Audio broadcasting, 118
Audio PLC modems, 138–139
Authentication
  EAP, 81–82
  IEEE 802.1x, 80
  PLC networks, 75
  public keys, 69
AZtech HomePlug AV Utility, 188

B

B2BIFS (beacon to beacon interframe spacing), 41
Back-off algorithm, 42–44
  back-off time, 42
  contention window size variation, 43
  random variable, 42
BIFS (burst interframe spacing), 41
Blocking filters, 147, 149
Blowfish, 65
BOOTP (Boot Strap Protocol), 238
BPL (broadband powerLine), 1, 151
Broadcast, 58

Broadcast address, 102
Brute force attacks, 72
Business PLC, 247–271
  access to electrical medium, 253–255
  application classes, 255
  architecture illustration, 249
  capacitive coupling, 253
  DHCP client configuration, 268–271
  DHCP/NAT server configuration, 269–270
  equipment placement, 255–256
  equipment selection, 251–256
  hotel implementation, 263–268
  inductive coupling, 253
  NAT (network address translation), 270–271
  network architecture, 248–250
  network architecture selection, 256–257
  network selection, 251–256
  repeater installation, 260–262
  security functionalities, 260
  security parameters, 257–260
  service quality, 252–253
  SNMP, 249–250
  standard selection, 250–251
  supervising, 249–250
  supervision tools, 250
  VoIP under, 262–263

C

Cables, 165
  length, 165–167
  types, 165
Cable TV modems, 134–136
  applications, 135–136
  compatibility, 136
  connectors, 135
  frequency bands, 134
Capacitance, 18–19
Capacitive coupling, 140, 253
CAP (channel access priority), 51, 52
CDCF (commonly distributed coordination function), 296
Cenélec, 1, 3, 6, 20, 24
CEN (European Standardization Committee), 3
Centralized mode, 36–38
  advantages/disadvantages, 32
  architecture, 37
  data communicated between devices, 37
  defined, 32
  devices, 37
  equipment, 129–130
  HomePlug AV, 129–130
  See also Network modes
CEPCA, 296–297
CIFS AV (contention distributed interframe spacing version AV), 41–42
CIFS (contention distributed interframe spacing), 40
Circuit breaker panel, 164–165
  defined, 164–165
  illustrated, 166
Coaxial cable, PLC over, 122
Community PLC, 273–293
  architecture, 280–282
  constraints, 280
  deployed networks, 289–293
  distribution networks, 279
  distribution network supervision architecture, 285
  Eichhoff injector connection, 282
  electrical network operators, 274–275
  electrical networks, 273–277
  electrical network topology, 275–276
  electrical subnet architecture, 274
  equipment selection, 283–284
  implementation, 277–293
  inter-POP backbones, 278
  issues in electrical networks, 282–283
  large-scale networks, 289
  local area networks (LANs), 279
  medium-scale networks, 288–289
  MV network topology, 276–277
  network configuration, 285–287
  NOC (Network Operation Center), 284
  position within network architecture, 278–280
  power line distribution system, 278
  power supply, 283
  small-scale networks, 287–288
  supervision, 284–285
  technology selection, 283–284
  very large networks, 278
Company standards, 5
Conductors, 165
Configuration, 179–216
  DHCP, 237–245
  DHCP client (Linux), 268–271
  DS2 network, 206–211
  HD-PLC network, 205–206
  HomePlug 1.0 network, 179–187
  HomePlug 1.0 network under Linux, 191–200

HomePlug AV network, 187–191
HomePlug AV network under Linux, 200–204
HomePlug Turbo network, 179–187
Internet gateway, 235–245
network parameters, 211–216
network parameters (Linux/BSD), 215–216
network parameters (Windows XP), 215
PLC gateway, 224–228
PLC network under FreeBSD, 204–205
PLC security, 228–230, 259–260
repeater, 261–262
Consortium standards, 5
Contention-free access (CFA), 53
Counterattacks, 61
Coupling, 140–141
capacitive, 140
direct tap, 143
inductive, 141
between phases, 21
Cryptography, 62–66
AES (Advanced Encryption Standard), 65–66
blowfish, 65
defined, 62
DES (Data Encryption Standard), 63–64
Diffie-Hellman, 67
IDEA (International Data Encryption Algorithm), 64
mixed-key, 68
principle, 62
public-key, 66–67
RC2, 64
RC4, 64
RC5, 65
RC6, 65
symmetric-key, 62–63
3-DES, 64
twofish, 65
See also Security
CSMA/CA (carrier sense multiple access/collision avoidance), 38–45
access to medium, 40–42
back-off algorithm, 42–44
data transmission example, 45
defined, 38
in HomePlug, 39
listening to medium, 39–40
CSMA/CD (carrier sense multiple access/collision detection), 38
Current Technology, 291–293

D

Data rates, 171–178
maximum, 175–177
PHY, estimating, 180
throughput calculation, 171–175
variation, 177–178
Decryption attacks, 79–80
De facto standards, 3
DEK (default encryption key)
defined, 180
network configuration with, 186
unique, 185
Denial of service (DoS) attacks, 71, 80
DES (Data Encryption Standard), 63–64
Devolo dLAN Software, 188
DHCP (dynamic host configuration protocol)
architecture, 239–245
architecture illustration, 240
client, dynamic configuration, 241
client configuration (Linux), 268–271
configuration, 237–245
configuration under Windows XP, 242–245
defined, 236, 238
parameters, 239–241
servers, 248
Dictionary attacks, 72
Diffie-Hellman, 67
Direct tap coupling, 143
Disturbance amplitude, 170
Domain name servers (DNS), 215, 236, 237
Double outlets, 171
DS2, 128
defined, 206
operation modes, 206
DS2 network configuration, 206–211
addressing planes, 207
HTTP tool, 207
multicast parameters, 210
PHY parameters, 210
PLC device MAC/network parameters, 208
PLC device network mode, 209
PLC device parameters, 208
security parameters, 210
Dynamic adaptation, bit rate, 58
Dynamic notching, 154

E

EAP (extensible authentication protocol), 80, 81–82
defined, 81

EAP (extensible authentication protocol) (continued)
EAP-MD5, 81
EAP-TLS, 81–82, 82
LEAP, 82
PEAP, 82
EAPoL (EAP over LAN), 82–83
EIFS (extended interface spacing), 41
Electrical networks
architecture, 15–24
attenuation on, 165–167
circuit breaker panel, 164–165
for communities, 273–277
distribution, simplified architecture, 17
electrical wiring, 17–22
interference effects, 169–171
issues in, 282–283
modeling, 22–24
MV (medium voltage), 151
operational responsibilities, 17
placing devices on, 220–223
single-phase wiring, 160, 161–163
three-phase wiring, 160, 163–164
topology, 160–168
voltage classification, 15, 16
wiring, 164
Electrical security, 217–219
Electrical wiring
attenuation, 20–21
capacitance, 18–19
characteristics, 17–24
coupling between phases, 21
electromagnetic noise, 19–20
frequency response, 21
impedance, 18, 19, 23
inductance, 18
interface sensitivity, 21–22
perturbations, 19–20
Electromagnetic compatibility, 157–160
Electromagnetic disturbances, 170
Electromagnetic noise, 19–20
Electromechanical meters, 145
Equipment, 125–150
business PLC placement, 255–256
capacitive coupling, 140
centralized mode, 129–130
community PLC, 283–284
cost, 148–150
direct tap coupling, 143
EMC requirements, 5
filters, 146–148
home PLC, 219–220
inductive coupling, 141
LV directives, 5
master-slave mode, 126–128
meters, 144–145
peer-to-peer mode, 128–129
PLC technologies, 125–130
repeaters, 145–146
signal injectors, 141–142
transformers, 143–144
transmission power, 158–160
Ethernet
device configuration, 183–187
modems, 133–134
PLC coexistence, 304
ETSI (European Telecommunications Standards Institute), 3, 6, 15, 20

F

FAIFA, 200, 201
File sharing, 116–117
Filters, 146–148
antinoise, 147, 149
blocking, 147, 149
cost, 150
Firewalls
hardware, 232
home PLC, 231–232
use illustration, 234
Fragmentation reassembly, 56–57
Frame check sequence (FCS), 49, 50
Frame level functionalities, 54–57
fragmentation reassembly, 56–57
MAC encapsulation, 55–56
Frames, 87–104
802.11b, 95
beacon, 51
control and management, 103–104
HomePlug, 95
MAC layer, 100–104
OFDM interface, 91–100
physical, access to, 75
physical, PLC, 96–100
physical layer, 88–90
priorities, managing, 51–52
FreeBSD, PLC network configuration, 204–205
FreeSWAN, 260
Frequency bands, 27–29, 151–160
cable TV, 134
disturbances, 154
dynamic notching, 154

electromagnetic compatibility and, 157–160
high bit rate, 155–157
illustrated, 153
low bit rate, 154–155
MV networks, 151
OFDM, 91
radio frequency regulation, 152–157
use for HomePlug AV devices, 93–94
Frequency response, 21
Functionalities, 31–60
dynamic adaptation of bit rate, 58
frame level, 54–57
network mode, 31–38
service quality, 59–60
transmission channel, 38–54
unicast, broadcast, multicast, 58–59

G

Gain/power correspondence, 159
Government standards, 5–6
GPS position, 286–287
Ground, 165

H

"The Handbook of Standardization," 4
Hash function, 69–72
defined, 69
with public-key cryptography, 70
HD-PLC network configuration, 205–206
Hexadecimal format, 102
Hi-fi quality telephony, 111
High-bit rate PLC, 155–157
Home-made PLC repeaters, 146, 147
Home PLC, 217–245
device placement on network, 220–223
electrical security, 217–219
equipment selection, 219–220
firewall, 231–232
Internet gateway configuration, 235–245
maximum number of devices, 230
PLC device placement, 222
PLC gateway configuration, 224–228
PPPoE tunnels, 233–235
RADIUS, 233, 234
security configuration, 228–230
security parameters, 223–235
technology selection, 219
testing operation, 230–231
VPNs, 232, 234
wiring diagram, 221
HomePlug
ACK acknowledgment, 47
architecture, 90
AV version, 41, 150
beacon frames, 51
centralized mode, 129–130
CSMA/CA in, 39
data link layer, 90
defined, 15
devices, frequency band use for, 93–94
evolution, 15
FAIL response, 49
frames, 95
frame structure, 88
frame synchronization, 50
frame time length, 88
frame times, 97
listening to medium, 40
long frame structure, 97
MAC frames, 100
NACK acknowledgment, 48
NEK (network encryption key), 73, 76
physical layer, 90
PLC modems, 132, 133
PLC network hierarchy, 36
SACK response, 49
security, 78
start delimiter details, 54
TDMA and, 44
Turbo, 149, 150
worldwide chip sales, 124
HomePlug 1.0 PLC configuration (Linux), 191–200
compilation parameters, 198
dmesg command, 194
Ethernet/USB virtual board, 197
installation command, 195
make install-boot command, 197
make install-usbdriver command, 196
make usbdriver command, 196
PLC configuration tool compilation, 199
PLC configuration tool installation, 199
PLC device sensing, 200
tool downloading window, 194
USB PLC device driver directory, 195
HomePlug 1.0/Turbo network configuration, 179–187
configuration tools, 181–182
Ethernet device, 183–187
parameters, 180
PHY data rate estimation, 180

HomePlug 1.0/Turbo network configuration (continued)
under Windows, 180–187
USB device, 183–187
visible parameters, 181
HomePlug Alliance, 8
HomePlug AV network configuration, 187–191
EasyConnect mode, 189
modes, 187–188
network interface choice, 189
Power Manager tool, 192
tool installation progress, 188
tool module installation choice, 190
tools, 188
HomePlug AV PLC network configuration (Linux), 200–204
FAIFA, 200, 201
integrated distribution tool, 200–201
Hotel PLC, 263–268
architecture illustration, 265
Internet access between computers, 268
logical architecture, 266
network architecture, 264
network implementation, 263–268
story, 266–267
story management, 267
story network architecture, 268
See also Business PLC
Hybrid PLC, 295–308
advantages/disadvantages, 304
multiple network coexistence, 295–304
optimized architecture example, 306–307
optimizing network architectures, 304–308
PLC and Wi-Fi coexistence, 298–303
PLC and wired Ethernet coexistence, 304
PLC technologies between themselves, 296–298
technology comparisons, 305

I

IDEA (International Data Encryption Algorithm), 64
IEC (International Electrotechnical Commission), 3, 7, 20
IEEE 802.1x, 80–84
architecture, 81
authentication, 80, 84
authentication server, 84
defined, 80
EAP authentication, 81–82
elements, 80
IEEE 802.11b frames, 95
IEEE 802.11 mode, 301
IEEE 802.3, 102–103
IEEE (Institute of Electrical and Electronics Engineers), 8–9, 15
defined, 8
future standard, 10
information resource distribution, 9
parties involved in standardization, 11
See also Standards
Impedance, 18, 19, 23
Inductance, 18
Inductive coupling, 141, 253, 256
Industry standards, 5
Installation, 151–178
Interface sensitivity, 21–22
Interference, 169–171
disturbances, 170
effects on electrical network, 169–171
Internet access providers (IAP), 217
InternetBox, 119–121
Internet connection
configuration, 235–245
dedicated computer, 236
DHCP, 236, 237–245
methods, 235
NAT, 236, 237–245
PLC modem-router, 237
sharing, 116, 236–237
Interoperability standard, future, 10
IP addresses, 211–212
IPsec, 85
IPv4 addresses, 212
ISO (International Standardization Organization), 3
ISRIC (International Special Radio Interference Committee), 20

K

KSA (Key Scheduling Algorithm), 64

L

Layered architecture, 27–29
frequency bands, 27–29
physical layer, 27
See also Architecture
Linksys PLE 200 Utility, 188
Linux

DHCP client configuration, 268–271
HomePlug 1.0 network configuration, 191–200
HomePlug AV network configuration, 200–204
network parameter configuration, 215–216
Local networks, 115–119
audio broadcasting, 118
file and printer sharing, 116–117
Internet connection sharing, 116
recreational applications, 118
video surveillance, 118–119
Wi-Fi network backbone, 119
See also PLC networks
Logical PLC repeaters, 27
Low bit rate PLC, 154–155
LV (low voltage) networks
branches, 277
topology, 276–277, 281

M

MAC address, 241
MAC encapsulation, 55–56
MAC layer frames, 100–104
address fields, 101–102
block check field, 100–102
control and management, 103–104
encrypted, format, 102–103
header format, 100–102
HomePlug 1.0, 100
Main.net, 127–128
Master-slave mode, 32–33
advantages/disadvantages, 32
architecture, 126
defined, 31
device manufacturers, 127–128
equipment, 126–128
equipment position, 127
master functionalities, 32–33
master PLC device functionalities, 33
technical solutions, 33
See also Network modes
MD2, 71
MD4, 71
MD5, 70, 71, 77–78
Meters, 144–145
EDF day/night tariff, 155
electromechanical, 145
use of, 144–145
MicroLink dLAN, 181
Mixed-key cryptograph, 68
Modeling
Cenélec and, 24
electrical devices, 23–24
electrical networks, 22–24
Modems, 130–140
audio, 138–139
cable TV, 134–136
cost, 150
dissipation in, 131
Ethernet, 133–134
HomePlug, 132, 133
integrated with electrical outlets, 136
LED indicators, 131
multifunction, 137–138
outside/inside illustration, 131
PLC/Wi-Fi, 136–137
telephone, 139–140
USB, 132–133, 134
use of, 131
See also Equipment
Motor vehicles, PLC in, 122–123
Multicast, 58
Multicast address, 102
Multifunction PLC modems, 137–138
Multimedia, 114–115
MV (medium voltage) electrical networks, 151
frequency band, 151
topology, 276–277
See also Electrical networks

N

NACK response, 46, 48
NAT (network address translation)
business PLC, 270–271
configuring, 237–245
defined, 236
routers, 237, 248
NEK (network encryption key), 73
calculating, 77
default, HomePlug, 76
defined, 180
in home PLC, 229
passwords, 185
for PLC logical network, 191
Network modes, 31–38
advantages/disadvantages, 32
centralized, 32, 36–38
functionality, 31–38
master-slave, 31, 32–33
peer-to-peer, 32, 34–36

Network parameters
address classes, 212–213
configuration, 211–216
configuration (Linux/BSD), 215–216
configuration (Windows XP), 215
DNS (domain name service), 214
IP addresses, 211–212
IPv4 addresses, 212
review, 211–214
subnet mask, 214
Neutral, 165
NOC (Network Operation Center), 284

O

OFDM (orthogonal frequency division multiplexing)
frequency bands, 91
functional blocks, 94–95
interface frames, 91–100
multichannel modulation, 158
symbol details, 92–93
symbols, 88, 91–93
transmission schemes, 92
Ohm's law, 19
Opera consortium, 9
Optimized architecture, 306–307
Overhead
maximal, 174
minimum, 173

P

Passive repeaters, 145
PCS (physical carrier sense), 52
Peer-to-peer mode, 34–36
advantages/disadvantages, 32
architecture, 34, 130
defined, 32
device parameters, 34–35
equipment, 128–129
parameter exchange in, 35
PLC network organization, 37
use of, 36
See also Network modes
Phase, 165
PHY data rate estimation, 180
Physical frames, 96–100
data body, 98, 99
elements, 96
end delimiter, 98–100
start delimiter, 98
Physical layer, 27
Physical layer frames, 88–90
Physical repeaters, 26–27
PLC
advantages/disadvantages, 10–12
for businesses, 247–271
for communities, 273–293
defined, 1
device priority, 180
functionalities, 31–60
in home, 217–245
hybrid, 295–308
InternetBox and, 119–121
modems, 130–140
in practice, 105–308
repeaters, 25–26
standardization, 10
technologies, 1–10
technologies in OSI model, 28
theory, 13–104
VoIP under, 262–263
PLC Forum, 10
PLC gateways
configuring, 224–228
data traffic priority levels, 227
elements determining, 224
for HomePlug device, 225
location of, 226
PLC networks
attacks, 78–80
authentication, 75
as backbones, 247
data rates, 171–178
development, 105
local, 115–119
network keys, 75–78
parameter configuration, 211–216
physical frames access, 75
physical medium access, 73–74
reliability, 72
security, 72–80, 178
security improvements, 80–85
simplicity, 72
status diagnostic function, 187
testing operation, 230–231
topology, choosing, 167–168
PLCP-PDU, 172
PLCP PPDU (physical level common protocol PPDU), 96
PLC/Wi-Fi, 298–303
device configuration, 300

hybrid architecture example, 299
modems, 136–137
optimized, 307–308
See also Wi-Fi
"Power line carriers," 2
Power line communications. *See* PLC
PowerPacket Utility, 181
Power strips, 171
PPPoE tunnels, 233–235
PRGA (Pseudorandom Generator Algorithm), 64
Printer sharing, 116–117
Private networks, 24–25, 26
Propagation, 168–169
PSD (power spectral density), 158
curve, 160
deviation, 159
maximum, 160
PSTN (public switched telephony network) model, 16
PUA (PLC Utilities Alliance), 9
Public-key cryptography, 66–67
defined, 66
hash function with, 70
illustrated, 67
key types, 66
RSA (Rivest, Shamir, Adelman), 67
See also Cryptograph
Public keys
authentication, 69
hash and, 71
use of, 69
Public networks, 24, 25
Pulsadis signal, 1, 155, 156

Q

QMP (QoS and MAC parameters), 253, 254
Quality of service (QoS), 51, 59
HomePlug AV, 252–253
management, 59
multimedia, 115

R

Radio frequencies
high bit rate PLC, 155–157
low bit rate PLC, 154–155
regulation, 152–157
RADIUS (remote authentication dial-in user service), 80, 82
defined, 82
diameter and, 81
home PLC, 233, 234
RC2, 64
RC4, 64
RC5, 65
RC6, 65
Reassembly, 57
Recreational applications, 118
Repeaters, 25–27, 145–146
active, 145
configuring, 261–262
cost, 150
defined, 145
home-made, 146, 147
installing, 260–261
logical, 27
passive, 145
physical, 26–27
PLC, 145–146
Resources, 309–311
books and articles, 311
Web sites, 309–311
RGIFS (reverse grant interframe spacing), 42
RIFS (response interface spacing), 41
Ripple Control, 1
RSA (Rivest, Shamir, Adelman), 67

S

SACK response, 49
Security, 61–85, 178
cryptography, 62–66
electronic signatures, 68–69
functionalities, 260
hash function, 69–72
holes, attacks on, 72
home PLC, 217–218, 228–230
HomePlug AV, 78
IEEE 802.1x and improvements to, 80–85
issues, 61–72
mixed-key cryptography, 68
for PLC networks, 72–80
public-key cryptography, 66–67
public keys, 69
topologies, 258–259
Security parameters (business PLC), 257–260
configuring, 259–260
topologies, 258–259
VLAN, 260
VPN, 260
Security parameters (home PLC), 223–235

Security parameters (home PLC) (continued)
configuring, 228–230
firewall, 231–232
PLC gateway, 224–228
testing operation, 230–231
VPN and PPPoE, 232–235
Segment bursting, 53–54
Shared medium architecture, 24–27
analogy with network hub, 25, 26
PLC repeater concept, 25–27
private networks, 24–25, 26
public networks, 24, 25
See also Architecture
SHA (Secure Hash Algorithm), 71
Signal injectors, 141–142
Single-phase wiring, 160, 161–163
defined, 160
topology illustrations, 162
See also Three-phase wiring
SNMP (simple network management protocol), 249–250
SoftPlug, 182
Speech packetization/depacketization, 109
Spidcom, 128
Spoofing attacks, 72
Standardization
consortiums and associations, 8–10
IEEE, parties involved in, 11
parties involved in, 7
towards, 10
Standards
company, 5
consortium, 5
de facto, 3
defined, 2, 3
government, 5–6
IEEE, future, 10
industry, 5
interoperability, future, 10
organizations, 2–4
types of, 4–8
voluntary, 4
Streaming, 112
Symmetric-key cryptography, 62–63
Synchronization
frame controls and, 49–51
HomePlug AV frames, 50–51

T

TCP/IP parameters, 243–245
of board via ipconfig, 245
configuring, 243
of LAN Ethernet board, 244
Telephone PLC modems, 139–140
Telephony over PLC, 108–114
capacity problems, 113–114
differentiating IP packets, 110–111
hi-fi quality, 111
speech packetization/depacketization, 109
streaming, 112
transit time, 110
video, 112
video routing rates, 113
Three-phase wiring, 160, 163–164
defined, 160
topology illustration, 163
See also Single-phase wiring
Throughput
calculation, 171–175
HomePlug Turbo PLC, 223
telephony, 223
Time division multiple access (TDMA), 13
beacon frames, 51
medium access in HomePlug AV and, 44
slots, 51
timeslots, 115
Tone map management, 52–53
Topology, 160–168
building dense urban area, 279
choosing, 167–168
electrical network, 275–276
LV network, 276–277, 281
mesh, 277
MV network, 276–277
ring, 277
security, 258–259
single-phase wiring, 160, 161–163
star, 276
three-phase wiring, 160, 163–164
Transfer time, 172
Transformers, 144
defined, 143
overriding, 144
Transit time, 110
Transmission channel
ARQ, 45–49
contention-free access, 53
CSMA/CA techniques, 38–45
defined, 38
frame priority management, 51–52
frequency channel management, 52–53
functionalities, 38–54
medium access, 38–45

Transmission channel (continued)
segment bursting, 53–54
synchronization and frame controls, 49–51
Transmission power, 158–160
Transmission time, 173, 175
3-DES, 64
Trojan horse attacks, 72
Twofish, 65

U

Unicast, 58–59
USB
device configuration, 183–187
modems, 132–133, 134

V

VCS (virtual carrier sense), 39, 52
VDSL bands, 304
Video, 112
routing, 113
surveillance, 118–119
Videoconferencing, 114
Virtual private networks (VPNs), 85
business PLC, 260
home PLC, 232, 234
Viruses, 72
Visioconferencing, 114
VLAN labels, 60
VLAN (virtual LAN), 260
VoIP, 262–263
Voluntary standards, 4

W

WANs (wide-area networks), 248
Wi-Fi
access point, 300
access point properties, 301
global configuration over, 301
network backbone, 119
optimized PLC, 307–308
PLC coexistence, 298–303
PLC hybrid architecture example, 299
Windows
DHCP configuration, 242–245
network connection window, 232
network parameter configuration, 215
PLC network configuration, 180–187
WinPCap tool, 227
Worms, 72

Z

Zyxel PLA, 188

Recent Titles in the Artech House Telecommunications Series

Vinton G. Cerf, Senior Series Editor

Access Networks: Technology and V5 Interfacing, Alex Gillespie

Achieving Global Information Networking, Eve L. Varma et al.

Advanced High-Frequency Radio Communications, Eric E. Johnson et al.

ATM Interworking in Broadband Wireless Applications, M. Sreetharan and S. Subramaniam

ATM Switches, Edwin R. Coover

ATM Switching Systems, Thomas M. Chen and Stephen S. Liu

Broadband Access Technology, Interfaces, and Management, Alex Gillespie

Broadband Local Loops for High-Speed Internet Access, Maurice Gagnaire

Broadband Networking: ATM, SDH, and SONET, Mike Sexton and Andy Reid

Broadband Telecommunications Technology, Second Edition, Byeong Lee, Minho Kang, and Jonghee Lee

The Business Case for Web-Based Training, Tammy Whalen and David Wright

The Business Privacy Law Handbook, Charles H. Kennedy

Centrex or PBX: The Impact of IP, John R. Abrahams and Mauro Lollo

Chinese Telecommunications Policy, Xu Yan and Douglas Pitt

Communication and Computing for Distributed Multimedia Systems, Guojun Lu

Communications Technology Guide for Business, Richard Downey, Seán Boland, and Phillip Walsh

Community Networks: Lessons from Blacksburg, Virginia, Second Edition, Andrew M. Cohill and Andrea Kavanaugh, editors

Component-Based Network System Engineering, Mark Norris, Rob Davis, and Alan Pengelly

Computer Telephony Integration, Second Edition, Rob Walters

Customer-Centered Telecommunications Services Marketing, Karen G. Strouse

Delay- and Disruption-Tolerant Networking, Stephen Farrell and Vinny Cahill

Deploying and Managing IP over WDM Networks, Joan Serrat and Alex Galis, editors

Desktop Encyclopedia of the Internet, Nathan J. Muller

Digital Clocks for Synchronization and Communications, Masami Kihara, Sadayasu Ono, and Pekka Eskelinen

Digital Modulation Techniques, Second Edition, Fuqin Xiong

E-Commerce Systems Architecture and Applications, Wasim E. Rajput

Engineering Internet QoS, Sanjay Jha and Mahbub Hassan

Error-Control Block Codes for Communications Engineers, L. H. Charles Lee

Essentials of Modern Telecommunications Systems, Nihal Kularatna and Dileeka Dias

FAX: Facsimile Technology and Systems, Third Edition, Kenneth R. McConnell, Dennis Bodson, and Stephen Urban

Fundamentals of Network Security, John E. Canavan

Gigabit Ethernet Technology and Applications, Mark Norris

The Great Telecom Meltdown, Fred R. Goldstein

Guide to ATM Systems and Technology, Mohammad A. Rahman

A Guide to the TCP/IP Protocol Suite, Floyd Wilder

Home Networking Technologies and Standards, Theodore B. Zahariadis

Implementing Value-Added Telecom Services, Johan Zuidweg

Information Superhighways Revisited: The Economics of Multimedia, Bruce Egan

Installation and Maintenance of SDH/SONET, ATM, xDSL, and Synchronization Networks, José M. Caballero et al.

Integrated Broadband Networks: TCP/IP, ATM, SDH/SONET, and WDM/Optics, Byeong Gi Lee and Woojune Kim

Internet E-mail: Protocols, Standards, and Implementation, Lawrence Hughes

Introduction to Telecommunications Network Engineering, Second Edition, Tarmo Anttalainen

Introduction to Telephones and Telephone Systems, Third Edition, A. Michael Noll

An Introduction to U.S. Telecommunications Law, Second Edition, Charles H. Kennedy

IP Convergence: The Next Revolution in Telecommunications, Nathan J. Muller

LANs to WANs: The Complete Management Guide, Nathan J. Muller

The Law and Regulation of Telecommunications Carriers, Henk Brands and Evan T. Leo

Litigating with Electronically Stored Information, Marian K. Riedy, Susman Beros and Kim Sperduto

Managing Internet-Driven Change in International Telecommunications, Rob Frieden

Marketing Telecommunications Services: New Approaches for a Changing Environment, Karen G. Strouse

Mission-Critical Network Planning, Matthew Liotine

Multimedia Communications Networks: Technologies and Services, Mallikarjun Tatipamula and Bhumip Khashnabish, editors

Next Generation Intelligent Networks, Johan Zuidweg

Open Source Software Law, Rod Dixon

Performance Evaluation of Communication Networks, Gary N. Higginbottom

Performance of TCP/IP over ATM Networks, Mahbub Hassan and Mohammed Atiquzzaman

The Physical Layer of Communications Systems, Richard A. Thompson, David Tipper, Prashant Krishnamurthy, and Joseph Kabara

Power Line Communications in Practice, Xavier Carcelle

Practical Guide for Implementing Secure Intranets and Extranets, Kaustubh M. Phaltankar

Practical Internet Law for Business, Kurt M. Saunders

Practical Multiservice LANs: ATM and RF Broadband, Ernest O. Tunmann

Principles of Modern Communications Technology, A. Michael Noll

A Professional's Guide to Data Communication in a TCP/IP World, E. Bryan Carne

Programmable Networks for IP Service Deployment, Alex Galis et al., editors

Protocol Management in Computer Networking, Philippe Byrnes

Pulse Code Modulation Systems Design, William N. Waggener

Reorganizing Data and Voice Networks: Communications Resourcing for Corporate Networks, Thomas R. Koehler

Security, Rights, and Liabilities in E-Commerce, Jeffrey H. Matsuura

Service Assurance for Voice over WiFi and 3G Networks, Richard Lau, Ram Khare, and William Y. Chang

Service Level Management for Enterprise Networks, Lundy Lewis

SIP: Understanding the Session Initiation Protocol, Second Edition, Alan B. Johnston

Smart Card Security and Applications, Second Edition, Mike Hendry

SNMP-Based ATM Network Management, Heng Pan

Spectrum Wars: The Policy and Technology Debate, Jennifer A. Manner

Strategic Management in Telecommunications, James K. Shaw

Strategies for Success in the New Telecommunications Marketplace, Karen G. Strouse

Successful Business Strategies Using Telecommunications Services, Martin F. Bartholomew

Telecommunications Cost Management, S. C. Strother

Telecommunications Department Management, Robert A. Gable

Telecommunications Deregulation and the Information Economy, Second Edition, James K. Shaw

Telecommunications Technology Handbook, Second Edition, Daniel Minoli

Telemetry Systems Engineering, Frank Carden, Russell Jedlicka, and Robert Henry

Telephone Switching Systems, Richard A. Thompson

Understanding Modern Telecommunications and the Information Superhighway, John G. Nellist and Elliott M. Gilbert

Understanding Networking Technology: Concepts, Terms, and Trends, Second Edition, Mark Norris

Understanding Voice over IP Security, Alan B. Johnston and David M. Piscitello

Videoconferencing and Videotelephony: Technology and Standards, Second Edition, Richard Schaphorst

Visual Telephony, Edward A. Daly and Kathleen J. Hansell

Wide-Area Data Network Performance Engineering, Robert G. Cole and Ravi Ramaswamy

Winning Telco Customers Using Marketing Databases, Rob Mattison

WLANs and WPANs towards 4G Wireless, Ramjee Prasad and Luis Muñoz

World-Class Telecommunications Service Development, Ellen P. Ward

For further information on these and other Artech House titles,
including previously considered out-of-print books now available through our In-Print-Forever® (IPF®) program, contact:

Artech House
685 Canton Street
Norwood, MA 02062
Phone: 781-769-9750
Fax: 781-769-6334
e-mail: artech@artechhouse.com

Artech House
46 Gillingham Street
London SW1V 1AH UK
Phone: +44 (0)20 7596-8750
Fax: +44 (0)20 7630-0166
e-mail: artech-uk@artechhouse.com

Find us on the World Wide Web at: www.artechhouse.com